GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

MEXICO

The FinFisher case

SonTusDatos
Cédric Laurant and Monserrat Laguna Osorio
sontusdatos.org

Introduction

The right to privacy is protected by the Mexican Constitution, which establishes that the privacy of one's person, family, residence, documents or possessions cannot be violated. In addition, the constitution recognises the human rights established in it, and those included in international treaties that Mexico has signed. However, it was not until 2007 that Mexico started to regulate the area of data protection: the constitution was amended in order to guarantee the right to data protection and established that any interference in communications must be approved by a judge. In July 2010, Congress enacted the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP). The scope of this law only applies to individuals and companies, not government and other public entities.

Policy and political background

The Federal Institute of Access to Information and Data Protection (IFAI) is the autonomous institution mandated to safeguard individual rights to data protection. In the beginning, IFAI only existed to guarantee the right of citizens to access government public information. However, since 2010 its mandate has been extended in order to guarantee the right to the protection of personal data.

In March 2013, Privacy International's report, The Right to Privacy in Mexico, Stakeholder Report Universal Periodic Review 17th Session,[1] pointed to concerns over surveillance practices. It highlighted that between 2011 and 2012, the Department of Defence bought USD 350 million worth of surveillance software to be used by the Mexican Army. Of concern here is the lack of transparency on the purchase and use of this software. Recent news also revealed that federal agencies had purchased software that might place individuals' right to privacy at risk.

Today there is doubt about whether Mexico has adequate laws and institutions to deal with any violation of their citizens' rights in terms of privacy and data protection, considering that the responsible party might be its own government.

FinFisher in Mexico

In March 2013, the Citizen Lab,[2] an interdisciplinary research centre at the University of Toronto, published an investigation about a spyware programme called FinFisher, marketed by the company Gamma International.

FinFisher is malicious software that requires the user to download fake updates from apparently reliable sources such as Adobe Flash, iTunes and BlackBerry. Once it is installed on a computer system, a third party can remotely control the user's computer and access it as soon as the device is connected to the internet. As soon as the device becomes infected by FinFisher, the hacker who used it is able to see the user's emails and social messaging conversations, take screenshots, obtain passwords, and switch on microphones and cameras. FinFisher cannot be easily detected by an antivirus or antispyware.

The Citizen Lab detected 25 countries with servers that host the programme.[3] In Mexico, an infected server was detected at the provider UNINET S.A. de C.V, while another was detected at IUSACELL S.A. de C.V., but in Malaysia where the company has some of its servers.[4]

Previously, reports had revealed that activists and members of political opposition around the world had their phones and computers tapped because they had been infected by FinFisher. For example, in February 2013, the European Centre for

1 Privacy International. (2013). *The Right to Privacy in Mexico, Stakeholder Report Universal Periodic Review 17th Session*. London: Privacy International. https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/mexico_stakeholder_report_-_privacy_international.pdf

2 The Citizen Lab's areas of investigation include human rights violations in the digital environment, censorship and surveillance. https://citizenlab.org

3 Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013). *You Only Click Twice: FinFisher's Global Proliferation*. Canada: The Citizen Lab. https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonlyclicktwice.pdf

4 Sánchez, J. (2013, July 17). Fijan plazo a UniNet y Iusacell para informar sobre FinFisher. *El Universal*. eleconomista.com.mx/tecnociencia/2013/07/17/fijan-plazo-uninet-iusacell-informar-sobre-finfisher

Constitutional and Human Rights (ECCHR), Reporters Without Borders, Privacy International, Bahrain Watch and the Bahrain Centre for Human Rights filed a complaint before the Organisation for Economic Co-operation and Development (OECD) against Gamma International with respect to it exporting espionage technology to Bahrain.[5] The software has been used to spy on activists in Bahrain. When asked about this, Gamma International declared that they only sell FinFisher to governments. However, they admitted to having found copies of their products and stolen demos that have been used in repressive regimes.[6]

On 20 June 2013, Mexican civil associations ContingenteMX, Propuesta Cívica and Al Consumidor filed a complaint with the IFAI that resulted in the authority investigating both IUSACELL and UNINET with the aim of learning about the use of FinFisher on their servers, and to protect the personal data that might be at risk. Academics, journalists, activists and members of civil society organisations joined the complaint.[7] A month later, Privacy International sent a letter to the IFAI supporting the investigation. The letter makes it clear that "the presence of a FinFisher Command and Control server in a country does not necessarily imply that this product is being used by Mexican intelligence or law enforcement authorities."[8] The ECCHR also supported the complaint by asking the IFAI to investigate the case.

At first, UNINET declared that they have no responsibility concerning the allocation of IP addresses assigned to clients, while IUSACELL claimed FinFisher was not installed on their servers.

On 3 July 2013, the Permanent Commission of the Mexican Congress exhorted the IFAI to begin the investigation, as requested by ContigenteMX, Propuesta Cívica and Al Consumidor.[9] Seven days later, Congress asked the Secretariat of the Interior for a detailed report on the state's strategy for monitoring cyberspace and how it avoids infringing on user privacy rights.[10] Congress also asked the Secretariat whether they had acquired the FinFisher software, and asked the Office of the Mexican Attorney General whether there had been any complaint about the wiretapping of individual communications. Neither has answered the questions.

On 11 July 2013, human rights activists from the group Civil Disobedience reported that they had found trails of the FinFisher programme on their mobile phones and computers and had received various, but undefined, threats.[11] The newspaper also reported that the Office of the Mexican Attorney General had spent nearly MXN 109 million (approximately USD 8 million) for the FinFisher software and about MXN 93 million (around USD 7 million) for a satellite tracking system called Hunter Punta Tracking/Locsys. Both purchases were made from the Mexican company Obses and, according to the newspaper *Reforma*, the contract was overpriced.

José Luis Ramírez Becerril, Obses's representative, declared that the company had sold the same espionage equipment to other Mexican government agencies. But if Gamma International only sells to governments and does not have resellers, how could Obses make the deal? Due to the initial legal procedure of verification that ContingenteMX, Propuesta Cívica and Al Consumidor filed against IUSACELL and UNINET to learn about the operation of FinFisher, the IFAI also decided to investigate Obses.

In its verification of Obses, which started in May 2013, the IFAI asked the company if it had sold the FinFisher software and had provided services to the government. The information it gave was insufficient as it argued that the information was protected by rules of confidentiality. The IFAI therefore imposed a fine of MXN 1,295,200 (approximately USD 100,200) on the company for obstructing the IFAI's investigation by not providing the full information it requested.[12]

There are records that show that, in August and September 2013, two citizens made two requests for information from the Secretariat of the Interior through the internet system INFOMEX, which is designed precisely for citizens to ask for

5 ECCHR, Reporters without Borders, Privacy International, Bahrain Watch, & Bahrain Center for Human Rights. (2013). *OECD Complaint against Gamma International for possible Violations of the OECD Guidelines for Multinational Enterprises*. United Kingdom: Privacy International. https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/jr_bundle_part_2_of_2.pdf

6 Vermer, A. (2013, July 22). Corruption scandal reveals use of FinFisher by Mexican authorities. *Privacy International*. www.privacyinternational.org/blog/corruption-scandal-reveals-use-of-finfisher-by-mexican-authorities

7 Ricaurte, P. (2013, June 28). IFAI: inicie investigación sobre FinFisher en México. *ContingenteMX*. contingentemx.net/2013/07/03/ifai-inicie-investigacion-sobre-finfisher-en-mexico

8 Ricaurte, P. (2013, July 3). Privacy International solicita al IFAI que inicie investigación sobre FinFisher. *ContingenteMX*. contingentemx.net/2013/07/03/privacy-international-solicita-al-ifai-que-inicie-investigacion-sobre-finfisher

9 Deputies Chamber. (2013). *Proposiciones con punto de acuerdo presentadas por diputado en la LXII Legislatura turnadas a comisión*. sitl.diputados.gob.mx/LXII_leg/proposiciones_por_pernplxii.php?iddipt=421&pert=4 .

10 *Ibid*.

11 Jiménez, B. (2013, July 11). Denuncian activistas cacería cibernética. *Reforma*. (Link only available for subscribers but available also at www.criteriohidalgo.com/notas.asp?id=180404)

12 IFAI. (2014). *Verification Process exp. PS.0025/13*. sontusdatos.org/biblioteca/decisiones-judiciales-y-administrativas

public information about the government. The first request asked for information about the use of the FinFisher software in government agencies.[13] The second request asked which strategies among those that entail eavesdropping on cyberspace had been implemented and, if this were the case, what the scope of the strategies were, including the protocols and rules that were used to avoid violating users' privacy.[14] The answer to both petitions was that the information requested did not exist and it was recommended that the specific agencies involved (the Army and the Attorney General) be asked.

On 4 September 2013, WikiLeaks revealed that executives from Gamma International visited Mexico in February and April 2013.[15] Carlos Gandini, high executive from that company, was in Mexico from 14 to 17 February, while Martin Muench, FinFisher developer, was in the country around 23 to 26 April. There is no information about what offices they visited. In September 2013, the Citizen Lab reported that the FinFisher command and control centres in the IP addresses that Citizen Lab had previously detected were still active: FinFisher was still installed and operating on the Mexican servers that Citizen Lab had reported on back in March 2013.[16] Since September 2013, there has been no new information about the presence of FinFisher on Mexican servers. On 4 August 2014, a hacker with the nickname of PhineasFisher announced that he had hacked FinFisher[17] and posted on the internet various confidential documents. Among these were what seem to be authentic client records, manuals, brochures, price lists and source code. According to a description of the leaked information,[18] it is interesting to note that, in the list of customers, the username "Cobham" appears, probably referring to the Cobham Group, whose division "Cobham Defence Electronics" builds products for defence, medical, industrial and commercial applications in Mexico.[19]

Analysis of the situation

Mexico has one single federal law regulating the area of privacy and data protection, the LFPDPPP. This law could be used against UNINET and IUSACELL because both are private parties that might be collecting and processing personal data illegally.[20] UNINET and IUSACELL must adhere to the principles of legality, consent, information, quality, purpose, fairness, proportionality and accountability under the LFPDPPP. This implies that both companies should have implemented adequate operational processes and information security measures in order to ensure the protection of those principles. In any transfer of personal data, the data owner[21] needs to be notified beforehand, unless the transfer is necessary or legally required to safeguard the public interest, or when required for a judicial proceeding.

In this regard, the constitution guarantees the individual's right to privacy and data protection, subject to a few exceptions, such as in the case of military invasion, serious breach of the peace, or any other event which may place society in severe danger or conflict. According to the constitution, only the federal judicial authority can authorise telephone wiretapping and the interception of private communications, at the request of the appropriate federal authority or the State Public Prosecution Service.

The IFAI's investigation is still in progress and it has not revealed any of its findings yet. The investigation addresses several issues: the cases in which FinFisher has been used, the purposes for which it has been used, and whether there has been due process. If FinFisher has been used by state entities to violate the communications of activists or the general population's human rights, with purposes different from the ones established under law, and the espionage has been carried out without any authorisation by the competent authorities, a serious violation of those constitutionally protected human rights is at stake.

In order to legally fight against this violation, one could initiate a judicial process called constitutional adjudication (*juicio de amparo*). This

13 INFOMEX. (2013). *No. application 0000400188713*. The application only can be seen as a result of a search in the Infomex system at https://www.infomex.org.mx/gobiernofederal/moduloPublico/moduloPublico.action

14 INFOMEX. (2013). *No. application 0000400230813*. The application only can be seen as a result of a search in the Infomex system at https://www.infomex.org.mx/gobiernofederal/moduloPublico/moduloPublico.action

15 Ramírez, P., & Molina, T. (2013, September 4). Desarrollador de FinFisher y otros ejecutivos del espionaje cibernético, activos en México, revela Wikileaks. *La Jornada*. wikileaks.jornada.com.mx/notas/desarrollador-de-finfisher-y-otros-ejecutivos-del-espionaje-cibernetico-activos-en-mexico-revela-wikileaks

16 Molina, T. (2013, October 7). Sigue activo el programa de espionaje cibernético FinFisher en México: Citizen Lab. *La Jornada.* wikileaks.jornada.com.mx/notas/sigue-activo-el-programa-de-espionaje-finfisher-en-mexico-citizen-lab

17 www.reddit.com/r/Anarchism/comments/2cjlop/gamma_international_leaked

18 pastebin.com/kZQ5Jojs

19 www.cobham.com/about-cobham/defence-systems/about-us/defence-electronics/san-diego/services/cobham-defence-electronics-mexico.aspx

20 By "processing" we mean the retrieval, use, disclosure or storage of personal data by any means.

21 The data owner is the individual to whom personal data relate.

process is mentioned in the constitution under a section entitled "Laws or acts issued by the authority, or omissions committed by the authority, which infringe the fundamental rights recognised and protected by this Constitution".[22] As the constitution protects the right to privacy, the legal basis upon which to file a constitutional adjudication would precisely be the violation of this human right and the absence of due process of law: the lack of a warrant by a judge authorising the interception of communications. A constitutional adjudication can also be founded on the rights protected under the international human rights treaties that Mexico has ratified. The jurisdiction that issues the decision of the constitutional adjudication is a federal court. Appeal of the ruling (*recurso de revisión*) is possible before an appeals court. As a last resort, it is the Supreme Court of Justice of the Nation (SCJN), Mexico's highest federal court, that is competent to hear the case, but only on a discretionary basis and if the matter is significant ("*asunto de importancia y transcendencia*"). In case the complaint is granted, whether at a federal court or before the SCJN, the court would restore the right claimed by the plaintiff, but not issue any sanction to the agency responsible for violating the right.

Another, completely different recourse would be to reclaim the patrimonial accountability (*responsabilidad patrimonial*) of the state. This is an administrative procedure, not a judicial one, which is designed for those individuals whose rights and property have been infringed on as a result of illegal or unconstitutional state administrative activity.[23] The judicial, legislative and executive branches of the federation, constitutional autonomous agencies, units, entities of the Federal Public Administration, the Office of the Mexican Attorney General, federal courts, administrative and any other public federal entity, are subject to this administrative procedure. A lawsuit of patrimonial accountability is presented before the offending agency and is aimed at determining if there was a fault – in this case, the violation of a human right. It is possible to appeal the agency's decision before the Federal Tax and Administrative Court. If the fault can be demonstrated and expressed in monetary terms, the plaintiff obtains relief through financial compensation.

The IFAI is responsible for guaranteeing the data owner's right to the protection of his or her personal data. In this case, however, its role is unclear. It can investigate, as it has already done, and issue fines. But there is no established procedure for a case of government surveillance. Also, as the matter at stake is a violation of human rights, another institution could play a role: the National Human Rights Commission (CNDH). Nevertheless, that institution may only make recommendations that are not binding: it can determine whether there was a violation of human rights and who was responsible, but can only issue recommendations to prevent it from happening again.

Conclusions

Mexico is facing a situation that is testing the strength of its legal framework and the effectiveness of its administrative and judicial institutions. The petition by ContigenteMX, Propuesta Cívica and Al Consumidor could prove to be a factor that triggers more complaints aimed at ensuring transparency and respect of human rights by the Mexican government – in particular with respect to the right to privacy.

No matter whether, one day or another, someone will demonstrate that the government used FinFisher and did it illegally, Mexico does have a legal framework in place that enables it to address the FinFisher case as a privacy violation and a breach of human rights. However, the country does not have the legal and institutional framework that enables it to tackle government surveillance cases effectively. Government espionage is a delicate issue because it is not always clear whether government authorities are acting to protect national security interests and whether they are going beyond their obligations and start infringing on citizens' human rights. It is precisely because limits are not always clear and institutions are fallible that there should be specific rules and procedures to safeguard individual human rights, as well as accountability and oversight rules that the government must comply with.

Action steps

There should be a minimum number of principles, the goal of which should be to protect the right to privacy and data protection, and to address government surveillance. Analysing the FinFisher case in light of existing legislation shows that the government is violating human rights, but is not revealing that it is spying on individuals, nor its seriousness. The International Principles on the Application of Human Rights to Communications Surveillance ("the Principles") are a good starting point to

22 Trife. (2013). *Mexican Constitution.* www.trife.gob.mx/sites/default/files/consultas/2012/04/cpeum_ingles_act_08_octubre_2013_pdf_19955.pdf

23 Cámara de Diputados. (2014). *Ley Federal de Responsabilidad Patrimonial del Estado*. www.diputados.gob.mx/LeyesBiblio/pdf/LFRPE.pdf

analyse other aspects of similar cases. These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology, and apply to surveillance conducted within a state or extraterritorially, regardless of the purpose of the surveillance.[24]

In order to guarantee privacy and data protection, ContingenteMX, Propuesta Cívica and Al Consumidor have also proposed that competent authorities reconcile their legal framework with the Principles.[25] However, the first seven of the 13 principles (legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority and due process) are in fact safeguards that can be found in the Mexican Constitution, which deals with human rights and the cases and circumstances in which the state is able to interfere with them. Then, it would be more important that the government commit to comply with the other six principles (user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access and right to effective remedy) because they provide propositions specifically focused on wiretapping communications in the surveillance ambit.

Aside from covering the legal aspect, it is also necessary to foresee the operative needs that the law requires to be enforced: there should be operative rules and procedures derived from the Principles that let the same principles work in practice. Then, once the government's commitment is verified, the state should determine the institutions and federal agencies that have to abide by those operative rules and procedures in order to protect individuals against surveillance. The compliance by the Federal Institute of Telecommunications (*Instituto Federal de Telecomunicaciones*) with the above-mentioned operative norms and procedures would, for instance, be necessary to guarantee the principles of user notification, but also the integrity of communications and systems. The Attorney General's Office (*Procuraduría General de la República*), on the other hand, would help implement the principles of legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority and due process. In fact, since all the principles are related to each other, every institution and federal agency that would commit to the objective of protecting individuals against surveillance would contribute to compliance with each of the 13 principles to various degrees. The state should also decide which specialised institution could guarantee the compliance with the applicable operative rules and procedures. In this sense, the IFAI is a good starting point because it is an autonomous institution that has a high level of public confidence. In this way, the principles of transparency and public oversight would be reinforced at the same time.

It is important to underline that the Principles would be worthless without an engaged society that demands respect of its rights. We recommend that from the Principles, we use the ones that can be promoted and exercised by Mexican civil society and non-profit organisations. As an example, the principle of legality suggests that, due to the rate of technological changes, limits to the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process. We recommend giving a role to civil society in these reviews. Regarding the principle of user notification, which establishes that individuals should be notified of communications surveillance, and the principle of transparency, which establishes that states should be transparent about communications surveillance, both of them can be achieved if civil society is vigilant and continuously informed about what the government is doing.

As a result, the action steps we recommend are the following:

- Establish a clear legal framework for using espionage software and other similar tools. There should be specific rules for when the government wishes to use software like FinFisher. The rules would indicate the cases in which it is allowed and how the privacy of all the individuals who are not being investigated is safeguarded.
- Ratify the United Nations Guidelines for the Regulation of Computerized Personal Data because, by doing so, individuals would be assured of obtaining a basic threshold of protection for their privacy and personal data. Mexico would also show its commitment towards better protecting individuals' communications and internet privacy.
- Encourage Congress to discuss the topic of government surveillance, as well as protect the privacy of communications.
- Organise campaigns to make civil society aware of the importance of privacy and how surveillance puts freedom of expression and association at risk.

24 https://en.necessaryandproportionate.org/text

25 Robles, J. (2013, October 7). Comunicado de prensa sobre los avances en las investigaciones sobre #Finfisher en Mexico. *ContingenteMX*. contingentemx.net/2013/10/07/comunicado-de-prensa-sobre-los-avances-en-las-investigaciones-sobre-finfisher-en-mexico