Mexico OGP Response Policy Concern Report

Approved by Criteria and Standards Subcommittee on 2 May 2019

I. Background:

On 16 July 2018, representatives of 10 civil society organizations that used to form part of the secretariat tasked to coordinate the Open Government Partnership (OGP) agenda in Mexico sent a Letter of Concern to the OGP Steering Committee regarding digital surveillance carried out by the Government of Mexico.[1] In particular, the Letter noted that individuals in organizations that have actively participated in the open government commitment building processes were among those targeted by malware attacks, alongside journalists, opposition figures, and other politically active Mexican citizens. The full Letter of Concern is attached as Annex 4.

Evidence of the attacks was first revealed by Citizen Lab, a Canadian-based research laboratory whose focus includes investigating digital espionage against civil society, in collaboration with Article19, SocialTIC and R3D, in February 2017.[2] In the aftermath of these reports, in May 2017 the Mexican civil society core group decided to quit its participation in the Third OGP Action Plan.

The Mexican government issued two official responses to the Letter of Complaint. The first was sent on 20 November 2018, by Dr. Eber Omar Betanzos Torres, on behalf of the government of then-President Enrique Peña Nieto. While the letter did not explicitly deny Mexican government involvement, it said that Citizen Lab's reporting had not established "conclusive evidence" of their responsibility for the cyber attacks. The letter also said that the Attorney General's Office (PGR) is investigating the matter, and that the Response Policy is not an appropriate venue for resolving complaints about these cyber attacks. The letter also proposed a roadmap to resume open government engagement with civil society.

The second response was issued on 31 January by Dr. Irma Eréndira Sandoval Ballesteros, on behalf of the government of President Andrés Manuel López Obrador, who assumed office in December. The letter was unclear as to whether, and to what degree, the government acknowledged that the allegations in the Letter of Concern were true. However, it specifically renounced surveillance attacks against civil society, journalists and opposition figures in Mexico, and announced a number of measures aimed at boosting transparency, oversight and accountability

---

[1] The complaint was signed by Ana Cristina Ruelas of Article19, Edna Jaime of the Centro de Investigación para el Desarrollo, Ernesto Gómez of Contraloría Ciudadana, Tomás Severino of Cultura Ecológica, Haydeé Pérez of Centro de Análisis e Investigación, Alejandro González of Agencia para el Desarrollo, Juan E. Pardinas of Instituto Mexicano para la Competitividad, Francisco Rivas of Observatorio Nacional Ciudadano, Juan Manuel Casanueva of SocialTIC, and Eduardo Bohórquez of Transparencia Mexicana. The Letter is attached as Annex 4, and is also available online: www.opengovpartnership.org/sites/default/files/Mexico_Response%20Policy_Mexican-Digital-Surveillance_July2018.pdf.

[2] John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, Citizen Lab, "BITTER SWEET: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links" (11 February 2017), online: citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

of surveillance activities. It also reiterated that the Attorney General was investigating what took place.

This Report was drafted as part of the OGP's Response Policy, which was initiated by the civil society Letter of Concern. The purpose of the Response Policy is to ensure that all participating countries uphold OGP values and principles, as expressed in OGP's foundational documents, specifically the Open Government Declaration and the Articles of Governance. According to the OGP Response Policy, the criteria for responding to a Letter of Concern is as follows:

1. Establish the veracity of the information by cross-referencing concerns with government, civil society, IRM researchers and third parties, including UN bodies, according to the nature of the issue.
2. Establish the relevance of the concern to the Open Government Declaration and OGP's Articles of Governance – i.e., is the matter being reported directly undermining fulfillment of the nation's commitment to OGP principles, thereby calling into question the process of its OGP participation.
3. Check with previous OGP data points, such as cross-referencing with the findings of the most recent IRM report on the country, including the national context section.
4. Assess whether an OGP intervention could have the desired impact in a country or is necessary to protect the credibility of OGP.[3]

After an initial review, the OGP Support Unit, in collaboration with, and under the oversight of, the Criteria and Standards (C&S) Co-Chairs, concluded that the concern meets the eligibility criteria to trigger a Response Policy inquiry, and hired a consultant to undertake a review of the Concern in accordance with procedures set out in Annex 2 to the Response Policy Procedures and Protocols *(Engaging External Assistance for Response Policy Cases)*. The process for this inquiry included reviewing OGP's Articles of Governance and the Open Government Declaration, cross-referencing the concern with recent IRM reporting for Mexico, and establishing the veracity of the information by reviewing civil society, government, media, and United Nations sources, as well as the responses received by the Government of Mexico. As part of this review, interviews were also carried out with the complainants and with representatives of the Government of Mexico, as well as with Citizen Lab. Having followed this process, the findings are as follows.

II. Relevance of the Complaint to the Open Government Partnership:

The Letter of Concern says that Mexico's conduct "has shown deep incongruencies in its actions and discourse regarding open government to the extent that it has undermined the current national open government progress and may likely undermine OGP's international credibility." The Letter of Concern also claims that, as a result of the surveillance, "safe and open spaces for civic society participation and criticism have been drastically reduced".

The impact of these allegations on the OGP process in Mexico is self-evident, insofar as civil society has viewed them as being sufficiently serious to warrant their withdrawal from participation in the Third Action Plan. In her 2017 Midterm Assessment Report, Gabriela Nava Campos, the Independent Reporting Mechanism (IRM) researcher for Mexico, noted a "critical"

[3] The Response Policy is included as Addendum F to the Articles of Governance, online: www.opengovpartnership.org/sites/default/files/attachments/OGP_Articles-Gov_Apr-21-2015.pdf.

need to restore trust and mechanisms of dialogue with civil society moving forward.[4] The issue was at the forefront of the IRM's recommendations included in that report: "Restore trust with civil society and strengthen governance of the OGP process in Mexico to guarantee its viability and consolidate its relevance."

However, even beyond the direct impact that these allegations have had on civil society's relationship with the government, the broader issue of surveillance, and the exposure of civil society to the threat of cyber attack, is highly relevant to the OGP. Constructive engagement with civil society is at the core of the OGP's mission, and its multistakeholder structure. Civic participation is one of the main OGP values, which in turn requires an enabling environment that is conducive to freedom of expression and freedom of association. This is spelled out in the Open Government Declaration: "We commit to protecting the ability of not-for-profit and civil society organizations to operate in ways consistent with our commitment to freedom of expression, association, and opinion."[5]

The nexus between privacy and freedom of expression and freedom of association, and the specific threat that intrusive surveillance poses to these rights, is well documented, including by the UN Special Rapporteur on Freedom of Expression:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy… Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.[6]

Speaking specifically of the cyber attacks that are the focus of the Letter of Concern, David Kaye, the UN Special Rapporteur on Freedom of Expression, and Edison Lanza, the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, said in a joint report:

> 52. A series of well-documented reports in 2017 demonstrated that the Government of Mexico and a number of state governments purchased or deployed software designed to monitor individuals through their mobile phones.
> …
> [S]urveillance technology has profound implications for the exercise of freedom of expression, undermining the ability of individuals to share or receive information and establish contacts with others. It creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information.[7]

---

[4] Gabriela Nava Campos, Open Government Partnership, "Mecanismo de Revisión Independiente (MRI): Informe de Avances de México, 2016-2018", online: www.opengovpartnership.org/sites/default/files/Mexico_Mid-Term_Report_2016-2018_Comments-Received.pdf.

[5] Open Government Partnership, "Open Government Declaration", online: www.opengovpartnership.org/open-government-declaration.

[6] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40, 17 April 2013, para. 79.

[7] IACHR & RFOE, Special Report on the Situation of Freedom of Expression in Mexico (June 2018), online: www.oas.org/en/iachr/expression/docs/2018_06_18_CIDH-UN_FINAL_MX_report_ENG.pdf.

In February 2018, Michel Forst, the United Nations Special Rapporteur on the situation of human rights defenders, issued a report on his visit to Mexico the previous year assessing the situation in that country. It also addressed the reports of digital surveillance:

> 41. Unsupervised secret surveillance of human rights defenders is a new and worrying challenge, especially in the context of weak judicial oversight regarding the collection, storage and sharing of personal data obtained through digital surveillance. After the visit, the federal and some state authorities were accused of purchasing and deploying spyware called "Pegasus" to monitor politicians, human rights defenders, journalists and lawyers through their mobile telephones. The Special Rapporteur reiterates his and other United Nations experts' call from July 2017 for an independent and impartial investigation to be carried out into the alleged illegal surveillance, which constitutes a serious violation of the rights to privacy and to the freedoms of expression and association. [references omitted][8]

In addition to posing a threat to the integrity of communications, the use of intrusive surveillance technology in Mexico raises very real physical security threats to its targets. Mexico is among the most dangerous places in the world to be a journalist or a human rights defender.[9] In at least one case, the cyber attacks were targeted in connection with an assassination.[10] In other words, the threat flowing from these attacks extends beyond operational concerns, and raises very real questions about the physical safety of those targeted, who in some cases have had to disrupt their lives and routines to deal with the potential danger they face.[11]

The allegations of surveillance against civil society and journalists, and in particular against organizations who are participating in the OGP process, is relevant to the values and principles of OGP. It is also worth noting that the Government of Mexico is a founding member of the OGP, and a current (2019) member of the Government Steering Committee. The prominence of Mexico within the OGP compounds the potential reputational risk stemming from these allegations.

The C&S Subcommittee finds that the Complaint is relevant to the OGP:

Surveillance and digital integrity are a core component of the rights to freedom of expression and freedom of association, and it is clear that the alleged activities have harmed civil society confidence in the OGP process, and their willingness and ability to

---

[8] UNHRC, Report of the Special Rapporteur on the situation of human rights defenders on his mission to Mexico, UN Doc. A/HRC/37/51/Add.2, 12 February 2018, online: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_51_Add_2_EN.docx.

[9] *Ibid.* See also Paola Nalvarte, Knight Center for Journalism in the Americas, "As murders of journalists rise globally, Mexico leads Latin America for media workers killed in 2018" (20 December 2018), online: knightcenter.utexas.edu/blog/00-20437-murders-journalists-rises-globally-mexico-leads-latin-america-professionals-killed-the.

[10] John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, Citizen Lab, "RECKLESS VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague" (27 November 2018), online: citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.

[11] Conversation with the civil society complainants, 18 February 2019.

engage. In addition, Mexico's prominence within OGP creates a substantial reputational risk if these allegations are not properly addressed.

III. Establishing the Veracity of the Complaint

In their official responses, the Government of Mexico neither confirmed nor denied that Mexican government agencies were responsible for the attacks, citing an ongoing investigation by Mexico's Attorney General. However, the new President, at least, has seemed to imply that he accepts that State agencies were culpable, including a statement on 19 December 2018 that the cyber attacks were "no longer" taking place, and another on 23 January 2019 that his government, "[is] not the same, it is not going to happen what they did to Carmen Aristegui, to Gutiérrez Vivó. No. Absolute, complete freedom of information and protection to the media."[12]

Attribution for cyber attacks is a notoriously tricky business.[13] However, Citizen Lab is at the global forefront of this field, particularly with regard to attacks against civil society. Their reporting establishes what could best be described as a strong circumstantial case for the Mexican Government's responsibility for the attacks.

The attacks are alleged to have been carried out using a form of software called "Pegasus", which is manufactured by the NSO Group, an Israeli company which, according to its statements, sells products only to "authorized governmental agencies".[14] Israeli media have previously reported that the Government of Mexico signed a deal to purchase $20 million dollars worth of NSO Group products in 2012.[15] Leaked information published from Hacking Team, an Italian surveillance malware vendor, is further suggestive of a connection between NSO Group products and Mexican buyers.[16] In June 2017, Enrique Peña Nieto, then President of Mexico, confirmed that his government had purchased Pegasus spyware.[17]

Citizen Lab has been researching NSO Group's products since at least 2016, when their software was used to attack Ahmed Mansoor, a prominent human rights activist based in the United Arab

---

[12] Both statements were included in the response letter from the Government of President Andrés Manuel López Obrador, as translated by the Consultant.

[13] See, for example, W. Earl Boerbert, "A Survey of Challenges in Attribution", in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S.Policy* (2010), online: www.nap.edu/read/12997/chapter/5.

[14] Thomas Brewster, Forbes, "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text" (25 August 2016), online: www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#61a4b0e33997.

[15] Orr Hirschauge, Haaretz, "U.S. Fund to Buy NSO and Its Smartphone-snooping Software" (17 February 2014), online: https://www.haaretz.com/israel-news/business/u-s-fund-to-buy-snooping-software-1.5323394.

[16] Wikileaks, "Hacking Team" (8 July 2015), online: wikileaks.org/hackingteam/emails/emailid/5391.

[17] Azam Ahmed, New York Times, "Mexican President Says Government Acquired Spyware but He Denies Misuse" (22 June 2017), online: www.nytimes.com/2017/06/22/world/americas/mexico-pena-nieto-hacking-pegasus.html.

Emirates (UAE).[18] Mr. Mansoor has been subjected to a number of different attacks, but the ones relevant to this case were delivered via SMS text messages to his phone.[19] The messages included a hyperlink which promised information about torture which was taking place in UAE jails, but which led to a website designed to implant malicious software on the visitor's phone. The malicious software would compromise all aspects of the device, allowing remote access to its camera and microphone, as well as access to other data stored on it. Citizen Lab was able to attribute the attack on Mr. Mansoor to NSO Group as a result of Internet Protocol address[20] information connected to the links which were sent to his phone. These addresses were connected to a server that had been registered by NSO Group. The malware itself also contained several hundred mentions of the term "_kPegasusProtocol".

Citizen Lab's investigations of the Mexico spyware attacks uncovered a similar pattern, which led them to conclude that they could also be traced to NSO Group. The Mexico spyware came in the form of SMS messages which attempted to "bait" the recipients into clicking on a link which would infect their phone.[21] While some of the messages included information related to the targets' work, such as false "breaking news" stories or notifications of a problem with the target's website, the attacks also included a number of crude sexual threats and accusations, as well as notices regarding the death of a family member or acquaintance. Citizen Lab found that the domains being used to host these attacks matched those which they had uncovered in their previous investigation of the attacks against Ahmed Mansoor, meaning that both attacks were carried out using the same online infrastructure.

Although Citizen Lab's reporting notes that it is impossible to conclusively attribute the attacks to the Mexican government, the facts strongly suggest that they are responsible.[22] The Mexican targets are drawn from a range of industries and sectors, including journalists, politicians, lawyers, and civil society activists who work on different causes. The common thread between them is that they are all active on issues which have a high profile in Mexico's domestic politics. The fact that Mexican government agencies are known as NSO Group customers is also important, as is the fact that NSO Group deals exclusively with governments, precluding the suggestion that the attacks were carried out by private sector actors, organized crime figures, or other independent parties. Finally, Citizen Lab's reporting points out that the targeting was very heavy handed, with some high profile subjects receiving a barrage of messages, including crude and highly provocative

---

[18] Amnesty International, "UAE: Activist Ahmed Mansoor sentenced to 10 years in prison for social media posts" (31 May 2018), online: www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/.

[19] Bill Marczak and John Scott-Railton, Citizen Lab, "THE MILLION DOLLAR DISSIDENT: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (24 August 2016), online: citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[20] An Internet Protocol address, usually abbreviated as an IP Address, is the distinct numerical label which is attached to every device connected to a computer network, giving it a unique identifier on that network.

[21] John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, Citizen Lab, "RECKLESS EXPLOIT: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware" (19 June 2017), online: citizenlab.ca/2017/06/reckless-exploit-mexico-nso/.

[22] John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, Citizen Lab, "BITTER SWEET: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links" (11 February 2017), online: citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.

taunts. This makes it unlikely to have been the work of a different government, as it would be extremely atypical to take such a brazen approach to attacks on foreign soil.

The C&S Subcommittee finds that the evidence supports the veracity of the complaint:

The attacks were carried out using a highly sophisticated tool which is only available to governments, and which the Mexican government is known is have purchased. The attacks targeted a range of victims, all of whom are prominent in Mexico's domestic politics, and were carried out in a manner which suggests that the perpetrator did not feel a particular concern about avoiding detection, as would typically be the case with foreign State actors. The Mexican government's responses to the allegations have alternated between evasive or vague denials, to tacit admissions of responsibility.

IV. Assessing the impact of an OGP intervention

In the months since the Letter of Concern was first filed, a number of important developments have taken place in Mexico. These include a change in government, with the election of Andrés Manuel López Obrador as the new President. As of February 2019, a tripartite consultation process, consisting of the government, civil society, and the Mexican Access to Information Institute (INAI), have begun meeting to discuss the establishment of a co-creation process to introduce new controls for accountability and transparency over the use of government surveillance. As of March 2019, the members of the former Tripartite Technical Secretariat formed a new coordination body called the "Coordination Committee", and have resumed the national OGP process in Mexico, and announced a timeline for addressing the issue of illegal state surveillance in Mexico.[23] Separate to this, the new administration has announced a number of initial measures aimed at preventing the abuses from happening again, such as enhanced transparency, including the declassification of material related to past illegal surveillance, and boosting the independence of the Attorney General, which was recently rechristened as the Fiscalía General de la República (FGR).

In conversations during the review process, civil society representatives noted these as positive moves.[24] At the time of research, it is clear that civil society is willing to re-engage for the development of Mexico's Fourth Action Plan, a process which is intended take place in parallel to the co-creation process aimed specifically at surveillance reforms. Nonetheless, civil society representatives note that the process of rebuilding trust will be a long one, which would require proper accountability as well as structural reform. Civil society emphasized the positive role that the OGP had played in drawing attention to this issue, acting as an "important pressure point" to

[23] Open Government Partnership, Mexico Resumes National Open Government Process, 5 March 2019, online: https://www.opengovpartnership.org/documents/mexico-resumes-national-open-government-process-march-5-2019

[24] Conversation with the civil society complainants, 18 February 2019.

push for a proper public response by the government.[25] Government representatives were equally positive on the OGP's role thus far, as a much needed "wake up call" which helped to shine a light on a serious issue.[26]

*** Criteria and Standards Interim Decision on the OGP Response Policy Case Concerning Mexico, 2 May 2019**

In line with the findings of the review report of the Response Policy case filed on 16 July 2018 concerning the Government of Mexico, the Criteria and Standards Subcommittee acknowledges that the Concern is relevant to the values and principles of OGP and that the evidence submitted by the filers supports the veracity of the Concern. Furthermore, in view of the acknowledgement on behalf of Mexican civil society and government representatives regarding the positive role that OGP has played in this issue, the Criteria and Standards Subcommittee recognizes that continued engagement on behalf of OGP is both warranted and welcomed by domestic actors.

The Criteria and Standards Subcommittee also recognizes the concurrent domestic efforts being led by the Coordination Committee of the OGP process in Mexico, including the development of a roadmap to tackle illegal state surveillance, the reinitiation of the national OGP process giving way to the co-creation of Mexico's Fourth National Action Plan (2019-2021), and fostering public dialogue regarding the issue of state or government surveillance in Mexico. It is worth noting that the timeline of activities included in the roadmap to address the problem of illegal state surveillance in Mexico do not conclude until August 2019.

In view of findings of the review report and acknowledging the timeline of domestic efforts taking place, the Criteria and Standards Subcommittee hereby resolves to maintain this Response Policy case active through the conclusion of activities included in the roadmap established to address the challenges that originally led to the filing of the Concern. The Criteria and Standards Subcommittee will, in coordination with representatives of the Coordination Committee, assess the progress made by the Government of Mexico through 31 August 2019 and determine if further intervention on behalf of OGP, if any, is warranted in line with the policies and procedures outlined in the Response Policy.

The Criteria and Standards Subcommittee will continue to provide outreach and support to the members of the Coordination Committee in Mexico, and calls on fellow Steering Committee members to support these efforts.

C&S final recommendation (forthcoming)

[25] *Ibid*.

[26] Conversation with the government representatives, 21 February 2019.

List of Annexes

Annex 1: Establishing the Relevance of the Concern to the Open Government Declaration and the OGP Articles of Governance

The C&S Subcommittee finds that the concern about intrusive government surveillance of civil society, and in particular of civil society participants in the OGP process, is relevant to the OGP's Articles of Governance, as well as the Open Government Declaration commitment to "support civic participation":

Letter of Concern	Relevant Citation
"In February 2017, evidence on the potential involvement of different Mexican government offices in illegal and disproportionated digital surveillance against at least three prominent research scientists and health advocates in Mexico was revealed by a technical report done by Citizen Lab with help of Mexican digital rights NGOs Article19, SocialTIC and R3D and reported by the New York Times. This attack targeted two individuals in organizations that have actively participated in the open government commitment building processes. … Dozens of Mexican and international organizations have condemned illegal government surveillance, including both the UN and OAS special rapporteurs on freedom of expression. Over one year later, the current administration has shown no political will to solve the problematic and the open government process with civil society is still broken. … We, as the civil society core group of organizations that have fostered and engaged with government OGPs processes in Mexico since its adoption, write this letter of concern as a last resource to help clarify and address the involvement of the Mexican government in the use of digital surveillance against Mexican civil society. We believe that the actions described in this letter are of the highest concern for Mexican civil society open and safe civic participation and directly affect OGP's reputation. Digital surveillance against civil society constitutes a direct threat to civic participation and is inconsistent to the basic principles of open government. Such actions directly affect the activities of civil society, the lives of individuals participating in civic spaces and the trust on the	**Open Government Declaration:** "We commit to protecting the ability of not-for-profit and civil society organizations to operate in ways consistent with our commitment to freedom of expression, association, and opinion. We commit to creating mechanisms to enable greater collaboration between governments and civil society organizations and businesses." **OGP Articles of Governance:** p. 2: "OGP provides an international forum for dialogue and sharing ideas and experience among governments, civil society organizations, and the private sector, all of which contribute to a common pursuit of open government." p. 3: "All OGP participating governments commit to meeting five common expectations. These are the following: … 3. Develop country action plans through a multistakeholder process, with the active engagement of citizens and civil society" p. 8: "Expectation of Steering Committee Members: SC members are expected to demonstrate their commitment to the principles of OGP through their participation in the international initiative and their domestic environment. They carry a special onus for leadership by example for the entire OGP community." Addendum F: OGP Response Policy p. 28: "To maintain the organization's credibility – and safeguard its long-term future – it is important that participating countries uphold OGP

government. It is impossible to establish any true and equal co-creation space in open government if civil society is being targeted illegally and disproportionately by digital surveillance. The civil society organizations that sign this letter have deeply questioned the Mexican government authorities real will to address the issues behind the most basic threats against secure and free citizen participation. We believe that Mexico, as one of the founding countries and current Steering Committee member should permanently uphold the values and principles expressed in the Open Government Declaration and in the Articles of Governance. The Mexican government has shown deep incongruencies in its actions and discourse regarding open government to the extent that it has undermined the current national open government progress and may likely undermine OGP's international credibility. Therefore, we ask you to take action under the Policy of "Upholding the Values and Principles of OGP, as articulated in the Open Government Declaration" adopted on September 25th 2014 aiming to: a) Assist a country in question to overcome difficulties and to help re-establish an environment for government and civil society collaboration, and b) Safeguard the Open Government Declaration and mitigate reputational risks to OGP. Civic space is what maintains open government real, true and effective. Any strategy, commitment and co-creation processes to build and maintain open government requires a safe, open and just civic space. In Mexico, safe and open spaces for civic society participation and criticism have been drastically reduced (see Annex for digital surveillance national context and Annex 3 for national context). The surveillance attacks against journalists, civil society leaders and human rights advocates are perverse, silent and sophisticated actions by the Mexican government to control, threaten and close citizen participation. And, the lack of actions to address such reality will only perpetrate impunity and foster a state of surveillance in the country.	values and principles, as expressed in the Open Government Declaration and in the Articles of Governance." p. 29: "This policy of reacting to actions that contradict the Open Government Declaration is thus designed to uphold the pre-existing commitments that OGP participating countries have made, but without imposing any additional requirements. The aim is to take actions that: a) Assist the country in question to overcome difficulties and to help re-establish an environment for government and civil society collaboration, and b) Safeguard the Open Government Declaration and mitigate reputational risks to OGP. … There are three main ways in which an inquiry can be triggered in the Criteria and Standards subcommittee under this response policy: … "3. The OGP Steering Committee or Support Unit receives a letter of concern from a civil society, not-for-profit organization, or media organization involved in OGP at the national or international level, including details on which country and why." p. 30: "Some of the types of issues that have been previously raised in concerns to the Steering Committee as damaging to the OGP process in a country may include (but are not limited to): … • Introduction of new/revised policies or actions that significantly reduce the space for non-governmental organizations to work independently, voice critiques, and/or receive funding from domestic or international sources (e.g. new NGO laws). • Introduction of new/revised policies, laws, or practices, or actions, that significantly reduce enjoyment of fundamental freedoms, notably freedoms of expression and peaceful assembly, and freedom to associate. • Introduction of new/revised policies or actions that significantly reduce online or offline media freedom, or threaten media ownership and independence." **Report of the Special Rapporteur on the promotion and protection of the right to**

We still believe in open government and the OGP platform. All negotiation, instances and dialogue with the Mexican open government process have been followed to address the issues stated in this letter. Despite the lack of significant advances since February 2017 and the broken trust between government and civil society, we identify the response policy as the last resource to address the deep crisis that open government process platform is currently living. We demand that OGP intervene in the country's situation so that dialogue, trust and co-creation can be achieved either with the current or the next government administration.”	**freedom of opinion and expression, UN Doc. A/HRC/23/40, 17 April 2013:** “States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy… Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States’ scrutiny” **IACHR & RFOE, Special Report on the Situation of Freedom of Expression in Mexico (June 2018):** “[S]urveillance technology has profound implications for the exercise of freedom of expression, undermining the ability of individuals to share or receive information and establish contacts with others. It creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information.”

Annex 2: Establishing the Veracity of the Claims:

Letter of Concern	Sources	Counter-arguments
"In February 2017, evidence on the potential involvement of different Mexican government offices in illegal and disproportionated digital surveillance against at least three prominent research scientists and health advocates in Mexico was revealed by a technical report done by Citizen Lab with help of Mexican digital rights NGOs Article19, SocialTIC and R3D and reported by the New York Times. This attack targeted two individuals in organizations that have actively participated in the open government commitment building processes. … In the months to follow, more surveillance cases were revealed becoming an international scandal. Dozens of Mexican and international organizations have condemned illegal government surveillance, including both the UN and OAS special rapporteurs on freedom of expression. Over one year later, the current administration has shown no political will to solve the problematic and the open government process with civil society is still broken. Scientific evidence and country in-depth surveillance reports indicate that the Mexican government offices purchase and use high-end technology against civil society and journalists without any public judicial evidence nor accountability frameworks to support it. As of August 30th 2017, technical proof has revealed that there have been over 100 infection attacks targeting 22 individuals including renowned journalist Carmen Aristegui and her son (then a minor), CEO of anti-	**Thomas Brewster, Forbes, "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text" (25 August 2016):** "NSO Group sent a statement to FORBES via email in which it said its mission was to make the world a safer place "by providing authorized governments with technology that helps them combat terror and crime". "The company sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations. Moreover, the company does NOT operate any of its systems; it is strictly a technology company," the statement continued." **Orr Hirschauge, Haaretz, "U.S. Fund to Buy NSO and Its Smartphone-snooping Software" (17 February 2014):** "In 2012 the Mexican government reported it had signed a $20 million deal with NSO." **Azam Ahmed, New York Times, "Mexican President Says Government Acquired Spyware but He Denies Misuse" (22 June 2017):** "At a press event, Mr. Peña Nieto acknowledged for the first time that his government had bought the sophisticated Israeli-made spyware, called Pegasus, but denied that it had ordered the surveillance." **John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, Citizen Lab, "BITTER SWEET: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links":**	**Response Letter from the Government of Enrique Peña Nieto:** "The Response Policy is not designed to resolve complaints about illegal surveillance, since said resolution corresponds to a judicial procedure currently underway carried out by the Attorney General's Office (PGR), the competent authority. According to CitizenLab's own reports, cited in The Letter of Concern, there is no jurisdictionally conclusive evidence on the facts alleged." [translated by the Consultant] **Response Letter from the Government of Andrés Manuel López Obrador:** "[O]n December 19, 2018 at a press conference, [President Obrador] stressed, in response to a question about the cases of espionage using Pegasus malware: "About espionage, that is no longer. You can now calmly talk on the phone. " … [R]egarding freedom of expression and respect for opponents President López Obrador said: "… We are not the same, it is not going to happen what they did to Carmen Aristegui, to Gutiérrez Vivó. No. Absolute, complete freedom of information and protection to the media." [translated by the Consultant]

corruption NGO IMCO and OGP member of the 1st Steering Committee Juan Pardinas, human rights lawyers and even the Interdisciplinary Group of Independent Experts sent by the Organization of the American States (OAS) to inquiry on the 2014 disappearances of 43 students in Iguala, Guerrero."	"This report describes an espionage operation using government-exclusive spyware to target a Mexican government food scientists and two public health advocates. The operation used spyware made by the NSO Group, an Israeli company that sells intrusion tools to remotely compromise mobile phones. On August 25, 2016, the Citizen Lab published a report showing that NSO's technology was used to target Ahmed Mansoor, a UAE-based human rights defender, as well as identifying targeting in Mexico. Mexico has previously confirmed that it is a purchaser of NSO Group's spyware. … The messages sent to Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación all contained links pointing to domains previously identified as part of our investigation into NSO's infrastructure. The URLs in several text messages directly linked to the exploit infrastructure, while in others targets received exploit links that were shortened using the bit.ly link shortening service. … While we do not conclusively demonstrate that elements of the Mexican government participated in the Bitter Sweet operation, circumstantial evidence suggests that this is a strong possibility. Only a government can purchase NSO's products: NSO Group explicitly limits the sales of its products to governments. Therefore, we can reasonably conclude that a government's NSO deployment was used in this attack. The Mexican Government is a confirmed NSO User: The Mexican government reported that it signed a $ 20 million dollar deal with NSO Group in 2012. Thus, elements of the Mexican government	

	likely had access to NSO products at the time of the Bitter Sweet operation. The targets work on multiple domestic Mexican issues: The same infrastructure used for the Bitter Sweet operation (the unonoticias[.]net domain) was also used to target a Mexican journalist who wrote a story about government corruption involving the Mexican President's wife and a high-speed rail contractor, among other domestic targeting. The targets of the Bitter Sweet operation work on issues related to soft drink consumption and parties outside Mexico may object to their work. A large multinational food and beverage company could conceivably have sufficient influence to encourage a different government that has purchased NSO to target Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación. However, it is not clear that another government would be equally interested in all of the other targets we have identified. Noisy targeting: The heavy handed targeting is also a factor suggesting that the Bitter Sweet operator is a Mexican governmental client: it is unlikely that a foreign country would use the NSO tool on Mexican soil so brazenly and so clearly risking discovery." **John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, Citizen Lab, "RECKLESS EXPLOIT: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware" (19 June 2017):** "This report expands the Mexican investigation and shows how 10 Mexican journalists and human rights defenders, one minor child, and one United States citizen, were targeted with NSO's Exploit Framework.	

	… The targets received SMS messages that included links to NSO exploits paired with troubling personal and sexual taunts, messages impersonating official communications by the Embassy of the United States in Mexico, fake AMBER Alerts, warnings of kidnappings, and other threats. The operation also included more mundane tactics, such as messages sending fake bills for phone services and sex-lines. Some targets only received a handful of texts, while others were barraged with dozens of messages over more than one and a half years. … Six Mexican journalists and television personalities received text messages with NSO links. The minor child of one journalist was also targeted. Five members of Mexican nongovernmental organizations also received such messages. The targets range across Mexico's political spectrum, and paint a picture of an effort to track key figures in Mexican media. … Staff and directors of two Mexican civil society organizations were also targeted using NSO exploit links: Centro Miguel Agustín Pro Juárez (Centro PRODH) and the Mexican institute for Competitiveness (IMCO)." **IACHR & RFOE, Special Report on the Situation of Freedom of Expression in Mexico (June 2018):** "52. A series of well-documented reports in 2017 demonstrated that the Government of Mexico and a number of state governments purchased or deployed software designed to monitor individuals through their mobile phones."	

Annex 3: List of Sources:

- Bill Marczak and John Scott-Railton, Citizen Lab, "THE MILLION DOLLAR DISSIDENT: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" (24 August 2016), online: citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.
- John Scott-Railton, Bill Marczak, Claudio Guarnieri, and Masashi Crete-Nishihata, Citizen Lab, "BITTER SWEET: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links" (11 February 2017), online: citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/.
- John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, Citizen Lab, "RECKLESS EXPLOIT: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware" (19 June 2017), online: citizenlab.ca/2017/06/reckless-exploit-mexico-nso/
- John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, Citizen Lab, "RECKLESS VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague" (27 November 2018), online: citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/.
- Gabriela Nava Campos, Open Government Partnership, "Mecanismo de Revisión Independiente (MRI): Informe de Avances de México, 2016-2018", online: www.opengovpartnership.org/sites/default/files/Mexico_Mid-Term_Report_2016-2018_Comments-Received.pdf.
- Open Government Partnership, "Open Government Declaration", online: www.opengovpartnership.org/open-government-declaration.
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40, 17 April 2013, para. 79.
- IACHR & RFOE, Special Report on the Situation of Freedom of Expression in Mexico (June 2018), online: www.oas.org/en/iachr/expression/docs/2018_06_18_CIDH-UN_FINAL_MX_report_ENG.pdf.
- Paola Nalvarte, Knight Center for Journalism in the Americas, "As murders of journalists rise globally, Mexico leads Latin America for media workers killed in 2018" (20 December 2018), online: knightcenter.utexas.edu/blog/00-20437-murders-journalists-rises-globally-mexico-leads-latin-america-professionals-killed-the.
- W. Earl Boerbert, "A Survey of Challenges in Attribution", in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S.Policy* (2010), online: www.nap.edu/read/12997/chapter/5.
- Thomas Brewster, Forbes, "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text" (25 August 2016), online: www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#61a4b0e33997.
- Orr Hirschauge, Haaretz, "U.S. Fund to Buy NSO and Its Smartphone-snooping Software" (17 February 2014), online: https://www.haaretz.com/israel-news/business/u-s-fund-to-buy-snooping-software-1.5323394.
- Wikileaks, "Hacking Team" (8 July 2015), online: wikileaks.org/hackingteam/emails/emailid/5391.
- Azam Ahmed, New York Times, "Mexican President Says Government Acquired Spyware but He Denies Misuse" (22 June 2017), online: www.nytimes.com/2017/06/22/world/americas/mexico-pena-nieto-hacking-pegasus.html.
- Amnesty International, "UAE: Activist Ahmed Mansoor sentenced to 10 years in prison for social media posts" (31 May 2018), online: www.amnesty.org/en/latest/news/2018/05/uae-activist-ahmed-mansoor-sentenced-to-10-years-in-prison-for-social-media-posts/.

- UNHRC, Report of the Special Rapporteur on the situation of human rights defenders on his mission to Mexico, UN Doc. A/HRC/37/51/Add.2, 12 February 2018, online: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_51_Add_2_EN.docx.

Interviews:

11 February 2019:

John Scott-Railton
Senior Researcher
Citizen Lab

18 February 2019:

Juan M. Casanueva
Founding Executive Director
SocialTIC

Alfredo Elizondo Rosales
Coordinador de Proyectos
GESOC A.C.

Andrea Castedo
Project Coordinator
Alianza para Gobierno Abierto

Tomás Severino
Director
Cultura Ecológica, A.C.

21 February 2019:

Dálida Acosta Pimentel
Head of the National Anticorruption System Linkage Unit

Gregorio Gonzalez Nava
General Director of Transparency

Eduardo Vargas Ortiz
Open Government Director

José Segundo Gómez Aguirre
Multilateral Affairs Director

Sandra Lizarraga
Representative from the Social Comptroller and Citizen Participation Unit

Arturo Ismael Estrada Vite
Executive Coordinator of the National Anticorruption System Linkage Unit

Annex 4: Letter of Concern:

Open Government Partnership
1110 Vermont Avenue NW
Suite 500/ Open Gov Hub Washington, DC 20005
United States

Letter of Concern

July 16th, 2018

Dear Members of the OGP Steering Committee,

In February 2017, evidence on the potential involvement of different Mexican government offices in illegal and disproportionated digital surveillance against at least three prominent research scientists and health advocates in Mexico was revealed by a technical report done by Citizen Lab with help of Mexican digital rights NGOs Article19, SocialTIC and R3D and reported by the New York Times. This attack targeted two individuals in organizations that have actively participated in the open government commitment building processes.

At the Mexican Open Government Secretariat meeting of February 16th, 2017, a letter signed by all 10 Mexican civil society organizations that lead the Open Government Partnership (OGP) actions in Mexico, was delivered to the Mexican government leads in OGP expressing profound preoccupation on government-lead surveillance on civil society, asking for an urgent inquiry on illegal surveillance against civil society and demanded that the Mexican Technical Tripartie Secretariat meeting proactively established the necessary efforts (such as an open government additional commitment) to enable regulation and transparency and accountability controls that can prevent illegal and disproportionate surveillance.

After 3 months of a lack of response from the Mexican authorities, on May 23rd 2017 the Mexican civil society core group decided to quit its participation in the 3rd Action Plan and the Tripartie Secretariat (see letter sent to the Mexican Government[1] and letter to OGP Steering Committee[2]). In the months to follow, more surveillance cases were revealed becoming an international scandal. Dozens of Mexican and international organizations have condemned illegal government surveillance, including both the UN and OAS special rapporteurs on freedom of expression. Over one year later, the current administration has shown no political will to solve the problematic and the open government process with civil society is still broken.

Scientific evidence and country in-depth surveillance reports indicate that the Mexican government offices purchase and use high-end technology against civil society and journalists without any public judicial evidence nor accountability frameworks to support it. As of August 30th 2017, technical proof has revealed that there have been over 100 infection attacks targeting 22 individuals including renowned journalist Carmen Aristegui and her son (then a minor), CEO of anti-corruption NGO IMCO and OGP member of the 1st Steering Committee Juan Pardinas, human rights lawyers and even the

[1] See letter sent to STT in May 23rd, 2017 in English (https://goo.gl/78q6tt) and Spanish (https://goo.gl/4nh8wM)
[2] See letter sent to OGP in May 23rd, 2017: https://goo.gl/hGGkfC

Interdisciplinary Group of Independent Experts sent by the Organization of the American States (OAS) to inquiry on the 2014 disappearances of 43 students in Iguala, Guerrero.

Different top Mexican government officials (including the President Enrique Peña Nieto) have addressed the issue in an erratic, late and light manner deeply breaking the most basic trust from civil society. In February 2017, no reaction was made by the executive branch, including the Secretary of Public Affairs and lead of the open government process. As more surveillance cases were made public in June 2017, the President's spokesman first denied the cases but days later the President himself publicly acknowledged the ownership of surveillance technologies, minimized the importance of surveillance and even threatened to prosecute those spreading rumors on the matter. The President withdrew his statement one day later.

In response to the legal case presented by several surveillance targets, the Attorney General's Office on Freedom of Expression publicly announced that they would lead the criminal inquiry but one year later no progress has been made. In late 2017 and early 2018, the Ministry of Public Affairs addressed the Mexican civil society with a proposal to resume dialogue and joint open government activities but failed to address the core civil society's demands on the issue: have the political will so that an in-depth inquiry on the surveillance cases can be done and establish a co-creation process that can identify and implement regulation that enables transparency and accountability controls that can prevent illegal and disproportionate surveillance in Mexico.

We, as the civil society core group of organizations that have fostered and engaged with government OGPs processes in Mexico since its adoption, write this letter of concern as a last resource to help clarify and address the involvement of the Mexican government in the use of digital surveillance against Mexican civil society. We believe that the actions described in this letter are of the highest concern for Mexican civil society open and safe civic participation and directly affect OGP's reputation.

Digital surveillance against civil society constitutes a direct threat to civic participation and is inconsistent to the basic principles of open government. Such actions directly affect the activities of civil society, the lives of individuals participating in civic spaces and the trust on the government. It is impossible to establish any true and equal co-creation space in open government if civil society is being targeted illegally and disproportionately by digital surveillance.

The civil society organizations that sign this letter have deeply questioned the Mexican government authorities real will to address the issues behind the most basic threats against secure and free citizen participation. We believe that Mexico, as one of the founding countries and current Steering Committee member should permanently uphold the values and principles expressed in the Open Government Declaration and in the Articles of Governance. The Mexican government has shown deep incongruencies in its actions and discourse regarding open government to the extent that it has undermined the current national open government progress and may likely undermine OGP's international credibility.

Therefore, we ask you to take action under the Policy of “Upholding the Values and Principles of OGP, as articulated in the Open Government Declaration” adopted on September 25th 2014 aiming to:

a) Assist a country in question to overcome difficulties and to help re-establish an environment for government and civil society collaboration, and
b) Safeguard the Open Government Declaration and mitigate reputational risks to OGP.

Civic space is what maintains open government real, true and effective. Any strategy, commitment and co-creation processes to build and maintain open government requires a safe, open and just civic

space. In Mexico, safe and open spaces for civic society participation and criticism have been drastically reduced (see Annex for digital surveillance national context and Annex 3 for national context). The surveillance attacks against journalists, civil society leaders and human rights advocates are perverse, silent and sophisticated actions by the Mexican government to control, threaten and close citizen participation. And, the lack of actions to address such reality will only perpetrate impunity and foster a state of surveillance in the country.

We still believe in open government and the OGP platform. All negotiation, instances and dialogue with the Mexican open government process have been followed to address the issues stated in this letter. Despite the lack of significant advances since February 2017 and the broken trust between government and civil society, we identify the response policy as the last resource to address the deep crisis that open government process platform is currently living. We demand that OGP intervene in the country's situation so that dialogue, trust and co-creation can be achieved either with the current or the next government administration.

Sincerely yours,

Ana Cristina Ruelas - Article19
Edna Jaime - CIDAC, Centro de Investigación para el Desarrollo Ernesto Gómez - Contraloría Ciudadana
Tomás Severino - Cultura Ecológica
Haydeé Pérez - Fundar, Centro de Análisis e Investigación Alejandro González - GESOC, Agencia para el Desarrollo
Juan E. Pardinas - IMCO, Instituto Mexicano para la Competitividad Francisco Rivas - Observatorio Nacional Ciudadano
Juan Manuel Casanueva - SocialTIC
Eduardo Bohórquez - Transparencia Mexicana

LETTER OF CONCERN ANNEX 1 - DIGITAL SURVEILLANCE USING NSO GROUP PEGASUS SPYWARE

In July and August 2016 at least three prominent Mexican health rights researchers and advocates, received suspicious SMS with malicious links while they were advocating to increase the soda tax in Mexico, improve consumer product labeling, and raise awareness of health risks associated with sugary drinks. These individuals are Dr. Simon Barquera, a researcher at Mexican Government's Instituto Nacional de Salud Pública (National Institute of Public Health), Alejandro Calvillo, Director of consumer rights and health advocacy NGO El Poder del Consumidor, and Luis Encarnación, Director of Coalición ContraPESO that works on obesity prevention.

These targeted individuals noticed that the text messages were provocative, personally directed and even threatening (see CitizenLab Report[3]). With concern they shared the text messages with Mexican digital rights and security NGOs SocialTIC and R3D who identified a similar attack pattern previously described by CitizenLab's August 25th 2016 report on NSO's technology that had been used to spy a renowned UAE rights advocate Ahmed Mansoor and Mexican investigative journalist Rafael Cabrera.[4] The technology used was created and sold by the NSO Group which has the capacity to silently exploit an iPhone and install the Pegasus spyware. The Pegasus spyware is known to be able to actively record or passively gather a variety of different data about the device. By giving full access to the phone's files, text and chat messages, microphone and video camera, the operator is able to turn the device into a silent digital spy in the target's pocket. This spyware can also access a wide range of personal data, such as calendar data and contact lists, as well as passwords, including Wi-Fi passwords. It is important to note that these attacks are targeted to specific individuals since Pegasus, as many other similar high-tech spyware, is sold under a licensing scheme where each infection unit is associated to a target.

The NSO Group is an Israeli "cyber war" company that sells sophisticated intrusion tools to "authorized governments with technology that helps them combat terror and crime". The NSO Group claims to obey "strict export control laws and regulations".[5] There is information that the Mexican government purchased NSO Group's spyware for 20 million USD in 2012.[6]

CitizenLab has identified that the most exploit infrastructure names are associated with Mexico, most probably used to attack Mexican targets. The other NSO exploit top infrastructure domains are from United Arab Emirates and Uzbekistan.[7]

SocialTIC and R3D requested CitizenLab's technical support in order to technically assess the attacks. After an in-depth analysis, CitizenLab published a report that identifies that the messages sent to Dr. Simon Barquera, Alejandro Calvillo, and Luis Encarnación all contained links pointing to domains previously identified as part of our investigation into NSO's infrastructure. The URLs in several text messages directly linked to exploit infrastructure.

On February 11th 2017, CitizenLab issued an in-depth report on the attacks on Barquera, Calvillo and Encarnación in which they describe the infection process in detail. Also, the New York Times published a story on this case on its front page where recalls the context of the attacks and highlights that "NSO emails leaked to The New York Times referred to multimillion-dollar, continuing NSO Group

[3] See full report: https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/
[4] See full report: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
[5] More information in https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional- spies-who-hacked-iphones-with-a-single-text/#6cf19ae73997
[6] See http://www.haaretz.com/israel-news/business/economy-finance/1.574805
[7] See infrastructre section at https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

contracts with several government agencies inside Mexico, and the Mexican government has been an enthusiastic buyer of foreign spy tools".[8]

On February 13th 2017, attacked Mexican NGOs El Poder del Consumidor and Coalición ContraPESO, alongside with Article19, R3D and SocialTIC, held a press conference and issued open letters visualizing these attacks and asking the Mexican Government for an explanation and an in-depth inquiry.[9] No public or official response from any Mexican Government office or official occurred.

At the Mexican Open Government Secretariat meeting of February 16th, 2017, a letter signed by all 10 Mexican civil society organizations that lead the open government partnership actions in Mexico, was delivered to the Mexican government leads in OGP (Arely Gómez from the Secretary of Public Function, Alejandra Lagunes of the National Digital Strategy Coordination at the President's office and all 7 commissioners of the Mexican Access to Information Institute - INAI) expressing profound preoccupation on government-lead surveillance on civil society, asking for an urgent inquiry on illegal surveillance against civil society and demanded that the Mexican OGP Secretariat proactively established the necessary efforts to enable regulation and transparency and accountability controls that can prevent illegal and disproportionate surveillance.[10] No public nor official response to address these issues was expressed by the Mexican Government or INAI at the time.

On June 19th 2017, CitizenLab's second technical report on new proven cases of Mexican individuals targeted with NSO Group's Pegasus spyware was made public.[11] New York Times published the story in it's front cover and Mexican NGOs held a press conference alongside the testimonies of surveillance victims.[12] The targets were renowned journalists, human rights and anti-corruption civil society specialists all working in different high-profile investigations, human rights abuse cases defense and anti-corruption initiatives. Mexican NGOs R3D, Article19 and SocialTIC published an in-depth report that described how the targets had been lured to click links with NSO malware exploits in specific timing linked to milestones of activity that could expose and challenge Mexican government authorities, including the president.[13]

Nine surveillance targets assisted by Digital Rights NGO R3D filed a joint formal criminal complaint at the Mexican General Attorney's Division on Crimes Against Freedom of Expression also on June 19th 2017.[14] This accusation started the formal criminal proceedings in compliance with Mexican law. In reaction, three days later, the Mexican President, Enrique Peña Nieto declared in a public event that the Mexican government does own surveillance technology, minimized the importance of surveillance against citizens, claimend the accusations to be false and threatened to file legal action against those "spreading false accusations".[15] Civil society organizations publicly condemned the President's statements as it, instead of aiming to defend people's right and basic legal due process, he explicitly limited a criminal investigation that had not even started and directly threatened civil society

[8] See full story: https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?_r=0
[9] See press release: http://elpoderdelconsumidor.org/saludnutricional/el-espionaje-del-gobierno-de-mexico-a-defensores-del-derecho- a-la-salud-no-debe-quedar-impune/
[10] See letter sent to the Mexican OGP Secretariat; https://goo.gl/z4reBU
[11] See CitizenLab full report: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ [12] See NYT full story: https://nyti.ms/2sGmhJ0
[13] See full #GobiernoEspía report: https://r3d.mx/gobiernoespia
[14] See accusation document sent to start the criminal inquiry: https://r3d.mx/wp-content/uploads/Denuncia-FEADLE-P%C3%BAblica.pdf
[15] See video: https://twitter.com/R3Dmx/status/878259101595090944

organizations and surveillance targets.[16] The next day, on June 23rd, the President publicly withdrew his previous statements highlighting that he would not prosecute those accusing the Mexican government of illegally surveilling journalists, activists and civil society members.[17]

On June 26th, the General Attorney's office made their criminal investigation plan public.[18] In response, civil society organizations responded with a public statement highlighting the plan's lack of detail and impartiality on the involvement of external technical advice and demanded that an international expert group be formed to give professional, non-bias and specialized oversight to the investigation.[19] This demand was never granted. Also, no official statement, collaboration or proactive action was done by the Ministry of Public Administration, which is the Mexican Government's lead at the Tripartite Secretariat, to support, drive or channel civil society's observations regarding the criminal investigation.

These surveillance revelations have outraged Mexican, Latin American and international organizations and prominent individuals. On February 14th 2017, a letter signed by leading digital rights, civic-technology and data organizations and technology groups was publicly shared. This case was showcased by CitizenLab at a plenary conference at the Internet Freedom Festival in March 2017.[20] And, on March 22nd, a letter signed by prominent public health specialists, scientists and organizations urged the Mexican president to “respect the values of freedom of expression, human rights and public health, investigate this situation in-depth and bringing justice”.[21]

As time passed and no advances were made in the criminal inquiry, international bodies focused on human rights have addressed the surveillance cases in Mexico as part of their country reports and declarations. On July 19th 2017, United Nations (UN) experts urged the Mexican Government to cease digital surveillance activity and to guarantee an impartial and independent investigation.[22] On December 4th 2017 and later on June 19th 2018, special rapporteurs on freedom of speech, David Keye (United Nations) and Edison Lanza (Organization of American States) on their joint visit to Mexico publicly asked the Mexican Government to guarantee the independence of the investigation.[23] Such claim has repeatedly been done by the victims and their lawyers as there is valid suspicion of the impartiality of the General Attorney's Office on an internal investigation as evidence shows that office was the one that purchased the NSO Group Pegasus malware.[24] And on March 2nd 2018 Human Rights special rapporteur Michael Frost addressed in his report from his 2017 visit to Mexico that illegal digital surveillance is worrisome under the Mexican context and it constitutes a violation to the right to privacy and the freedom of expression and association.[25]

[16] See public statement by civil society organizations: http://centroprodh.org.mx/index.php?option=com_content&view=article&id=2404:2017-06-23-00-19-01&catid=209:front-rokstories&lang=es
[17] See video of the President’s statements: https://www.youtube.com/watch?v=vOVJ_9tx2lU&feature=youtu.be [18] See full statement from the Attrorney General’s office: https://twitter.com/PGR_mx/status/879405294337441792
[19] See full response: https://socialtic.org/blog/organizaciones-responde-a-feadle-de-la-pgr-sobre-espionaje/ [20] See IFF 2017 program https://internetfreedomfestival.org/schedule/ and session documentation https://internetfreedomfestival.org/wiki/index.php/Investigating_and_defending_against_Malware_Operations [21] See support letter: http://elpoderdelconsumidor.org/comunidad-internacional-vs-espionaje/
[22] See OHCHR press release: https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=S
[23] See Mexico’s preliminary report http://hchr.org.mx/images/doc_pub/ES-final-version-preliminary-observations.pdf and final report http://hchr.org.mx/images/doc_pub/20180618_CIDH-UN-FINAL-MX_reportSPA.pdf
[24] See journalistic report on the purchase of the Pegasus malware https://contralacorrupcion.mx/pegasus-pgr/
[25] See Human Rights Council 37th session agenda http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session37/Documents/A_HRC_37_51_Add_2_EN.do cx

At a national level, Mexican authorities have done very little to address the issue and the demands of the victims and civil society organizations. The only formal approach was done on May 28th 2018 when a Mexican Federal Judge ordered the Attorney General Office to seriously attend the surveillance case inquiry, including to include in the investigation the proof that the victims and their lawyers included in the case since the start of the criminal investigation.[26]

More so, over a month after the OGP Steering Committee delegation visit to Mexico in October 2017, the Ministry of Public Administration open government team only sent a superficial work proposal to the civil society group in open government.[27] This proposal aimed to achieve a legal framework analysis and an attention protocol for illegal surveillance victims but did not address how the Mexican Government would try to improve the ongoing inquiry nor established any commitments that would enforce transparency, accountability and legal measures on illegal digital surveillance against citizens. [28] The only collaboration on the matter linked to the original Mexican open government Tripartite Secretariat is a working group between the Mexican Access to Information Institute (INAI) and different civil society organizations (R3D, Article19 and SocialTIC) that since early 2018 aims to analyze how transparency and access to information policies have been applied to surveillance and personal communications interventions in Mexico.

[26] See Mexican civil society press brief:
https://r3d.mx/wp-content/uploads/GobiernoEspia-comunicado-audiencia-21MAYO.pdf
[27] See the civil society group public communication at the OGP Steering Committe visit to Mexico in October 19th 2017: https://gobiernoabiertomx.org/blog/2017/10/19/posicionamiento-del-nucleo-ante-la-visita-de-visita-de-mision-del-c omite-directivo-de-ogp/
See the OGP Steering Committee Delegation report after its visit to Mexico in October 2017:
https://www.opengovpartnership.org/sites/default/files/OGP-SC-Envoys_Visit-Mexico_October2017.pdf
[28] See the Ministry of Public Administration letter and work proposal of December 5th 2017: https://goo.gl/9Movuo (letter) and https://goo.gl/psbdMa (work plan)
See civil society group response in December 14th 2017: https://goo.gl/sVFLWk

LETTER OF CONCERN ANNEX 2 - DIGITAL SURVEILLANCE MEXICAN CONTEXT

Mexico has a worrisome digital surveillance history. Despite the lack of transparency from the Mexican government and the technical complexity that comes with identifying top-end spyware technology, there is now a track record that links the previous and current government administrations to the illegal purchases and use of highly intrusive technology such as the ones sold by Gamma International (ei. FinFisher spyware), Hacking Team (ei. Da Vinci and Galileo remote control systems) and NSO Group (ei. Pegasus spyware). Government digital surveillance has increased without following national laws, public explanations nor controls that can avoid its unlawful use against civil society. Local digital rights NGO Red para los Derechos Digitales (R3D) 2016's report on Surveillance in Mexico has defined the situation as "out of control".[29]

In 2012 civil society warned on potential use of a very sophisticated and highly intrusive spyware technology sold by FinFisher against activists in Mexico. That concern was reinforced by Privacy International's 2013 report, The Right to Privacy in Mexico, revealing that between 2011 and 2012, the Mexican Department of Defense had bought surveillance technology for USD 350 million.[30] But the lack of transparency by the Mexican government nor army never clarified details of such purchases and how these tools were being used.

Further inquiries from civil society and involvement of different government institutions regarding the use of FinFisher in Mexico is detailed in Hivos and APC's report "Global Information Society Watch 2014" where they highlight that in June 2013 Mexican civil society organizations ContingenteMX, Propuesta Cívica and Al Consumidor filled an inquiry to the National Access to Information Institute (IFAI) and asked the Ministry of the Interior for a detailed report on the government's strategy on digital monitoring and their privacy rights policies. The debate was also taken to the Mexican Congress who determined to also ask the Ministry of Interior if 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.

The main consequence after these inquiries was that a private company had bought the spyware technology on behalf of government institutions. IFAI imposed a fine of approximately USD $100,200 to the company for obstructing the IFAI's investigation by not providing the full information it requested. The "Global Information Society Watch 2014" report on Mexico highlights that "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.[31]

In July 2015, WikiLeaks exposed hacked emails from surveillance vendor Hacking Team. That information revealed that the Mexican government was the top buyer worldwide with purchases of over 5.8 million Euros.[32] Further inquiries linked Hacking Team malware purchases to a wide diversity of Mexican government offices, the vast majority were not legally authorized to buy and use surveillance technology.[33] The Mexican Minister of Interior tried to link Hacking Team purchases to the

[29] See full report: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf
[30] See full report: http://catedraunescodh.unam.mx/catedra/EPU/images/stories/Informes_Pendientes/21-%20PI.pdf [31] See full report: http://giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf [32] See leaked source: https://wikileaks.org/hackingteam/emails/
[33] See Hacking Team activity in LATAM in Derechos Digitales Surveillance Report: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

previous administration even though records show that payments were done in both administrations, even after the was a presidential change.[34]

As much of top-end surveillance technology, Hacking Team's products are technically very difficult to detect, assess and track. One visible case of illegal use of such malware was flagged in the state of Puebla where it was identified as the source for surveillance against local independent journalist and political opposition.[35]

As pointed out earlier in this letter, in CitizenLab's report of August 24th 2016, the use of spyware from Israeli cyber-ware company NSO Groups technically details how the Trident iOS exploit had been used to infect with the highly intrusive Pegasus malware the phones of UAE Human Rights Defender Ahmed Mansoor. The report highlights a similar attack to Mexican investigative journalist Rafael Cabrera, renowned for reporting the multi-million dollar scandal of the conflict of interest involving the President and First Lady of Mexico known as *La Casa Blanca*. [36]

In late 2016, Mexican digital rights specialists R3D published an in-depth report on surveillance in Mexico which analyzes current legislation, judicial interpretations and reflectionbased on the known surveillance practices in the country. This report is based on an extensive access to information exercise and an thorough analysis on the Mexican legal framework.[37] They conclude that:

1. The Mexican legal framework lacks democratic controls enabling government authorities to surveil anyone without controls, transparency or accountability

2. Most surveillance actions have been done without any judicial authorization and / or control

3. The known use of surveillance activity has not delivered penal outcomes as most cases of surveilled people are not sent to trial

4. Access to information and transparency mechanisms are not useful in practice do to the government's resistance to open information on surveillance and when information was granted by government authorities, judges and companies it was found to be incomplete or even contradictory.

[34] See reporting by Animal Político: http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/
[35] See reporting by Animal Político: http://www.animalpolitico.com/2015/07/el-gobiernode-puebla-uso-el-software-de-hacking-team-para-espionaje-po litico/
[36] See CitizenLab Report https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ and investigative journalism revelations http://aristeguinoticias.com/0911/mexico/la-casa-blanca-de-enrique-pena-nieto/
[37] See full report: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf This report was done with suppor of Internews, OSF and Privacy International

LETTER OF CONCERN ANNEX 3 - MEXICAN CONTEXT ON HUMAN RIGHTS, VIOLENCE AND FREEDOM OF EXPRESSION

The illegal surveillance against Mexican civil society, journalists, academia and human rights advocates is engraved under Mexico's increasing corruption, impunity, violence and human rights violations. Despite the legislative reforms and institutional progress, Mexico's civic space continues to shrink as it lacks to guarantee safe, open and reliable institutional support for its citizens.

In April 2015, the General Transparency and Access to Public Information Law was published strengthening 2002's legislation as it increased access to information guarantees and its applicability beyond the executive branch of government. Furthermore, the National Institute for Access to Information and Personal Data Protection (INAI) gained the power to intercede unconstitutional actions against laws that threaten or limit the access to information and personal data protection rights.[38] This reform gave INAI constitutional autonomy making its decisions definite and unassailable.

Nevertheless, several laws criminalize citizens that search for information have been set especially when inquiries are being done over public officers or addressed what can be vaguely identified as "national security".[39] Many access to information requests that have been appealed as they oppose international standards and conventions, especially those aiming for transparency in grave human rights violations and corruption. For instance, INAI recently reserved information regarding the Odebrecht-Pemex corruption case.[40] There are 20 restrictive legal law initiatives and four operational laws associated with crimes against honor, anti-protest and even, against the publication of memes.[41]

Regarding accountability, in April 2015 constitutional reforms were passed to create the National Anticorruption System (SNA) which should coordinate and homologate actions and policy in three government levels (federal, state and municipal) in the prevention, detection and sanction of corruption cases. Nevertheless, the implementation of this policy has been delayed by the Legislative and to this date it still lacks the nomination of the country's Anticorruption Prosecutor. Nevertheless, Mexico has continuing falling places reaching in 2017 the 135th position in Transparency International 2017's Corruption Perception Index.[42]

Mexico is in a severe violence and security crisis, and the lack of any institutional progress significantly worsened by the lack of access to justice and a state of almost total impunity. Seventeen states of the country, that is, more than half are in red hot spots for high-impact crimes. Baja California Sur, Colima, Zacatecas, Guanajuato, Querétaro, Aguascalientes and Tabasco stood out this year due to the levels of insecurity that they registered. In a rate per 100,000 inhabitants, they are located in the top 5 places of homicide, kidnapping, extortion and robbery.

In human rights matters, the constitutional reforms of 2011 recognized the government's obligation to comply to international human rights principles and laws. Nevertheless, civic space and its three core liberties (association, expression and assembly) have reduced in the past years. The National

[38] The current general law now identifies political parties, labor unions, public trust funds and other fund management organizations, the executive, legislative and judicial branches of government and institutions and people that recieve or spend public resources or participate in public actions.
[39] See Article19's analysis on criminalization of citizen information requests: https://eljuegodelacorte.nexos.com.mx/?p=5740
[40] More information on INAI's ruling of the Odebrecht-Pemex access to information case: http://www.economiahoy.mx/energia-mexico/noticias/8481476/07/17/El-INAI-reserva-la-informacion-del-caso-OdebrechtPemex.html
[41] See Article19 assessment on restrictive laws in Mexico: https://mapa.articulo19.org/#!/principal/2017/
[42] See full report: https://www.transparency.org/news/feature/corruption_perceptions_index_2017

Registry for Disappeared Persons (RNPED) accounts for 33,482 disappearances.[43] According to Article19, 111 journalists have been murdered since 2000 of which 38 journalist murders have been committed within the current government administration and reaching an impunity rate of over 99%. Additionally, aggressions against journalists have increased by 23% only in 2017 making it the most mortal year against the press.[44]

Freedom of assembly is constantly attacked as it's common to witness break-ins of strategic offices and spaces, threats and attacks against human rights advocates, the increase and lack of derogation of restrictive laws, public shaming of civil society organizations and human rights advocates, as well as targeted civil society organizations are being restricted to become registered charities. In Mexico, there is a daily attack against a human rights advocates, leaders and CSO personnel.[45] In peaceful gatherings, illegal use of force such as tear gas, use of metal bourne weapons, police encapsulation, and illegal incarceration against protesters have been used.

Furthermore, the government has increased military involvement in public safety responsibilities increasing violence and human rights violations maintaining opacity and lack of accountability. In December 2017, the Interior Security Law was bluntly passed which enables the President to authorize military intervention in police duties when "interior security threats" are identified and the federal or local capacities are insufficient to address "the threat". The law was passed despite national and international opposition including the United Nations High Commissioner for Human Rights, over 250 Mexican civil society organizations and academics, the INAI, the National Human Rights Commission, all State Human Rights Commissions and the majority of the state Access to Information Councils.[46] The unconstitutionality of this law is currently being appealed in the Supreme Court.

[43] More detail with focus on forced disappearances, extrajudicial executions, torture, access to justice, violence against the press and human rights advocates is available on the Interamerican Human Rights Council's report. See http://www.oas.org/es/cidh/informes/pdfs/mexico2016-es.pdf

[44] See Article19's latest report on violence against freedom of the press in Mexico: https://articulo19.org/informesemestral2017/

[45] See: http://www.proceso.com.mx/513092/en-mexico-ataque-al-dia-contra-defensoras-derechos-humanos-rnddhm

[46] See: www.seguridadsinguerra.org and https://www.forbes.com.mx/organizaciones-alrededor-del-mundo-declaran-en-contra-de-la-ley-de-seguridad-interior/