5 October 2020

Ms. Mary Lawlor,
Special Rapporteur on the situation of human rights defenders,
Office of the United Nations High Commissioner for Human Rights,
United Nations Office at Geneva
defenders@ohchr.org

Dear Ms. Lawlor,

We are writing to express our support to your mandate and to welcome the new call for inputs to inform your thematic studies to be presented at the Human Rights Council in its March session and at the General Assembly in October.[1]

Privacy International (PI) [2] is a London based registered charity that works globally[3] at the intersection of modern technologies and rights. We challenge overreaching state and corporate surveillance, so that people everywhere can have greater security and freedom through greater personal privacy. We are fighting for a world where technology will empower and enable us, not exploit our data for profit and power.

We appreciate your intention to focus on the pressing issue of killings of human rights defenders. The increasingly and continually escalating dangers human rights defenders face across the globe pose not only a threat to their lives, but they also threaten the autonomy, dignity and integrity of the communities whose human rights those same defenders have been acting to promote or protect. As you state in the concept note "there is no more direct attack on civil society than the murders of human rights defenders".

[1] https://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/CFI-killings-human-rights-defenders.aspx
[2] www.privacyinternational.org
[3] https://privacyinternational.org/where-we-work

In your call for inputs you indicate that you intend to report on the issue of killings of human rights defenders, as well as the threats of killings from State and non-State actors and, among others, "identify and explore effective preventive and protection measures and lessons learnt in the protection of human rights defenders". You aim to "provide a platform for dialogue between stakeholders to share experiences".

In light of this call, PI is writing to kindly suggest covering in your upcoming reports the impact that surveillance – and as such the role of serious and systematic interferences with the right to privacy of human rights defenders –contributes to the killings of human rights defenders across the world.

Indeed, the reported numbers of human rights defenders killed are rising, however, we have noticed that often what is less reported is the role that communications surveillance plays in facilitating those killings. And this is despite existing evidence that the surveillance of specific individuals including human rights defenders has been shown to lead to arbitrary detention, sometimes to torture and possibly to extrajudicial killings.[4]

Below we provide a few examples of such instances which have been well-documented which illustrate why this is a matter of urgency for your mandate to consider in this report.

Kenya

In 2017, PI issued a report revealing how intelligence gained by intercepting phone communications, primarily by the Kenyan National Intelligence Service (NIS), is regularly provided to units of the Kenyan police to carry out counter-terrorism operations, particularly the GSU-Recce company, the reconnaissance company of the General Services Unit (GSU), a paramilitary force officially under the Kenya Police Service Control, and the Anti-Terrorism Police Unit (ATPU).[5]

Officers of the GSU-Recce Company have admitted to carrying out extrajudicial killings as a matter of policy. ATPU officers have also been linked to extrajudicial disappearances. A senior officer recalls: "The person who will be having the information is the person who has been doing the surveillance, who is NIS. So they will give the first briefing."[6]

The NIS appears to have direct access to communications networks - meaning that they can access the information flowing through a network without the network operators' knowledge and they also have equipment that allows the interception of mobile communications. Communications

[4] https://undocs.org/A/HRC/41/35
[5] https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf
[6] https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya

surveillance is being carried out by Kenyan State actors, essentially without oversight, outside of the procedures required by Kenyan laws.[7]

You can find further information in our full report available on our website[8] and also attached as annex to this letter (Annex 1).

Intercepted communications content and data are used to facilitate serious human rights abuses, to spy on, locate, track and ultimately arrest, kill or disappear suspects. By ensuring that surveillance is lawful, necessary and proportionate with respect to privacy, we can effectively protect the lives of HRDs and ensure they can continue to fulfil their work safely and securely.[9]

Mexico

Several instances have been documented in which surveillance, and in particular surveillance malware tools, has been used against human rights defenders as well as dissidents and journalists in Mexico.[10] Due to the covert nature of these operations, it is often difficult to make direct connections between surveillance and follow-up threats to those targeted. However, lack of evidence *stricto sensu* should not be automatically considered as not existing.

You can find further information on the threats faced by HRDs in Mexico as enabled by communication surveillance in our Universal Period Review stakeholder report available on our website[11] and also attached as annex to this letter (Annex 2)

Chile

In the case of Chile, we are concerned about the indiscriminate and constant surveillance of specific groups, such as Mapuche indigenous communities, as well as those who advocate for their rights, through the abusive use of telecommunications interception mechanisms, geolocation tracking, and the use of surveillance drones.[12]

It has been reported that the anti-terror law which allows for communication surveillance, amongst other measures, is being used by government agencies such as the "the Jungle Commando", a

[7] https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf
[8] https://privacyinternational.org/report/43/track-capture-kill-inside-communications-surveillance-and-counterterrorism-kenya
[9] https://privacyinternational.org/case-study/3316/it-can-protect-our-lives
[10] https://privacyinternational.org/sites/default/files/2018-08/UPR_The%20Right%20to%20Privacy%20in%20the%20%20United%20Mexican%20States.pdf
[11] https://privacyinternational.org/sites/default/files/2018-08/UPR_The%20Right%20to%20Privacy%20in%20the%20%20United%20Mexican%20States.pdf
[12] https://privacyinternational.org/advocacy/2511/el-derecho-la-privacidad-en-chile

tactical unit of the national police force created by the Pinera government in 2018, to intimidate, silence and control the Mapuche.[13]

You can find further information in our Universal Period Review stakeholder report available on our website[14] and also attached as annex to this letter (Annex 3).

Colombia

Communications interception scandals (sometimes called by the Colombian Spanish term 'chuzadas') have been a feature of Colombian security politics since the 1990s. They include the unlawful surveillance of human rights defenders as well as families of disappeared persons, politicians, judges and journalists.

In 2014, the Colombian weekly magazine Semana reported that a Colombian army unit codenamed Andromeda was spying for more than a year on the government's negotiating team in ongoing peace talks with the country's FARC guerrillas.[15] Different agencies have been reportedly involved in these illegal interceptions such as the military-police Unified Action Groups for Personal Liberty (Grupos de Acción Unificada por la Libertad Personal, GAULA) targeting 2,5000 phone lines including of the Association for the Relatives of Detained-Disappeared (ASFADDES), a group representing the families of the disappeared, among many other human rights organisations.[16]

The most notorious of the interception scandals involves the Administrative Department of Security (DAS) and was revealed by Semana in February 2009. Special strategic intelligence groups of the DAS conducted targeted surveillance of an estimated 600 public figures including parliamentarians, journalists, human rights activists and lawyers, and judges among others. According to files retrieved during an investigation by the Fiscalía, the DAS intercepted phone calls, email traffic and international and national contacts lists, using this information to compile psychological profiles of targets and conduct physical surveillance of subjects and their families, including children.[17] Communications surveillance was central to the DAS abuses.

[13] https://www.aljazeera.com/opinions/2019/12/4/what-is-behind-state-violence-in-chile/; https://www.hrw.org/report/2004/10/27/undue-process/terrorism-trials-military-courts-and-mapuche-southern-chile
[14] https://privacyinternational.org/advocacy/2511/el-derecho-la-privacidad-en-chile
[15] http://www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/37607
[16] http://www.acnur.org/t3/leadmin/scripts/doc.php?le=t3/uploads/media/COI_53
[17] http://www.eltiempo.com/archivo/documento/CMS-543604

You can find further information in our Universal Period Review stakeholder report and available on our website[18] and also attached as annex to this letter (Annex 3), and our submission to the Human Rights Committee available on our website[19] and also attached as annex to this letter (Annex 4).

Defending dissent and the right to freedom of assembly

These are not isolated incidences. The year 2019 was marked by the reporting that an invasive spyware - known as Pegasus – produced by the Israeli firm NSO Group that was used, according to WhatsApp, to target more than 100 human rights activists. The spyware exploited a WhatsApp vulnerability that allowed attackers to inject commercial spyware on to phones simply by ringing the number of a target's device. The messaging app is often used by human rights defenders around the world.[20]

The instances highlighted here are just a few of the cases which have been well-documented. There are so many more which remain unreported, unknown, and unaccounted for. The limited publicly available information does not reflect the true scope and breadth of the precarious increasingly perilous situation faced by HRDs as are result of being subject to surveillance.

Sophisticated surveillance technology is used by governments across the globe facilitate the targeting, arrest and oppression of anyone participating in peaceful uprisings, dissent or criticise their actions.

Serious and systematic interferences with their right to privacy, on the one hand, should be considered as a factor that facilitates the targeting of human rights defenders. On the other, the protection of their right to privacy should be understood as an effective preventive and protection measure.[21]

We hope that you will consider addressing the issues we had highlighted in this letter in your report and/or that you would consider dedicating future thematic reports on surveillance as an impediment to their work, and a threat to their lives.

[18] https://privacyinternational.org/advocacy/2511/el-derecho-la-privacidad-en-chile
[19] https://privacyinternational.org/press-release/1326/colombias-record-privacy-surveillance-and-human-rights-under-renewed-scrutiny
[20] https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/ One example such example: https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/
[21] https://privacyinternational.org/long-read/2852/protecting-civic-spaces

Please don't hesitate to reach out if we can be of any assistance at all, both for the drafting of these reports or future work.

We are looking forward to engaging collaboratively and constructively with your mandate.

Yours sincerely,

Kuda Hove
Policy Officer
Protecting the targeted Project Lead

Dr. Ilia Siatitsa
Programme Director
Protecting civic spaces Project lead
Privacy International