Joint Report on the Situation of Human Rights Defenders in the Americas

Questionnaire prepared by the Office of the UN High Commissioner for Human Rights and the Inter-American Commission on Human Rights

May 2019

The Office of the UN High Commissioner for Human Rights (OHCHR) and the Inter-American Commission on Human Rights (IACHR) invite you to share information on the situation of human rights defenders in the Americas. The information gathered through this questionnaire will contribute to the joint OHCHR-IACHR report on the subject, which will be launched late in 2019.

This report will be publicly available on the website of OHCHR and on the website of the IACHR.

Your responses will be made public and attributed to you in the report, unless you indicate otherwise. Where possible please limit the response to each question to 500 words.

National Human Rights Institutions, civil society and human rights defenders are invited to send their responses in Word format by e-mail to adesouza@ohchr.org with an address where they can receive a reply to their submissions if necessary. For this purpose, a downloadable version of the questionnaire in English, French and Spanish is available on the OHCHR website.

The deadline for submitting the completed questionnaire is **10 June 2019.**

Please provide your contact details in case we need to contact you regarding this questionnaire. (Note that this is optional).

- Name of the organisation/institution:
- Electronic Frontier Foundation

- Contact and e-mail:
- Danny O'Brien, Directory of Strategy, danny@eff.org.

- Country or sub-region (indicate the country or sub-region in which you work)
- We work globally, with particular attention paid to the United States, and Latin America.

- Can we attribute these responses to you or your organization publicly?
- Yes.

Questions:

- **Situation of human rights defenders:**

What do you consider to be the contextual factors - positive and/or negative - that have had the greatest impact on the situation of human rights defenders in your country and/or region since 2016?

Our particular attention is on the rise of the use of cybercrime law to target human rights defenders who use technology either as their primary tool to communicate human rights concerns to the public or as a means to enable others to exercise their human rights through technology. This is especially true in relation to technologists working to defend people's right to privacy in the digital age. We are concerned with the targeting of technologists for their work as technologists who work to protect human rights in the digital age, in the same way that journalists and lawyers with human rights issues are frequently targeted for harassment or state-led detention or threats, despite their role being legitimate and lawful.

EFF has been concerned with this targeting since our founding in 1990, and we have opposed in the courts the prosecution or intimidation of technologists, particularly digital security experts, in the United States since this time (see https://www.eff.org/issues/coders).

We have previously noted the use of cybercrime laws to intimidate or prosecute human rights defenders in regions outside the Americas, for instance, within the Middle East (see https://www.eff.org/deeplinks/2016/04/crime-speech).

In the last three years, we have become concerned of the spread of such prosecutions in the Americas outside of the United States, most pressingly with the current prosecution of Ola Bini, a Swedish security researcher currently being detained in Ecuador. (see https://freeolabini.org/). We see this as a flagship case indicating the growing seriousness of this issue in the region.

What are the main causes and/or risk situations that contribute to a situation of violence and vulnerability against human rights defenders?

For this class of human rights defenders, we find two primary issues: the ambiguity and broad interpretation of cybercrime laws in multiple states in the region, and the increasing exploitation of public concerns about the dangers of modern technology and negative media depictions of dangerous "hackers" to discredit human rights defenders, separate from the due process they deserve.

For the first issue, please see our 2018 report, "Protecting Security Researchers' Rights in the Americas", https://www.eff.org/coders-rights-americas and (PDF) https://www.eff.org/deeplinks/2018/10/canada-chile-security-researchers-have-rights-our-new-report, which outlines human rights standards that lawmakers, judges, and the Inter-American Commission on Human Rights, can use to protect the

fundamental rights of security researchers.

For the second issue, we can point to the chain of events associated with security researcher Ola Bini. Bini's arrest was preceded by a press conference, and framed as part of a process of defending Ecuador from retaliation by associates of Wikileaks. During the interview, Ecuador's Interior Minister announced that the government was about to apprehend individuals who are supposedly involved in trying to establish a piracy center in Ecuador, including two Russian hackers, a Wikileaks collaborator, and a person close to Julian Assange. She stated: "We are not going to allow Ecuador to become a hacking center, and we cannot allow illegal activities to take place in the country, either to harm Ecuadorian citizens or those from other countries or any government." However, neither she nor any investigative authority has provided any evidence to back these claims.

Following the arrest, the National Police of Ecuador announced on Twitter that "through the use of digital platforms of social networks, the subject transmitted information of social connotation (disclosure of information) through websites, among the most prominent, Wikileaks. The subject used false profiles." This announcement was accompanied by a photograph of books and devices that had been confiscated from Ola's home and himself. While this tweet was later deleted, it contributed to the media impression that Ola Bini was a malicious hacker.

(See https://freeolabini.org/en/timeline-ola/ and https://www.eff.org/deeplinks/2019/04/free-ola-bini)

In fact, Ola Bini is a free software developer, who works to improve the security and privacy of the Internet for all its users. He has contributed to several key open source projects used to maintain the infrastructure of public Internet services, including JRuby, several Ruby libraries, as well as multiple implementations of the secure and open communication protocol OTR. Ola's team at ThoughtWorks contributed to Certbot, the EFF-managed tool that has provided strong encryption for millions of websites around the world.

The so-called "evidence" seized from Ola's home that Ecuadorean police showed journalists to demonstrate his guilt was nothing more than a pile of USB drives, hard drives, two-factor authentication keys, and technical manuals: all familiar property for anyone working in Ola's field as well as any tech-savvy user who understands technology. Prosecutors have, as yet, provided no evidence to indicate Bini was a threat to Ecuador, but continue to hold him in arbitrary detention.

This is typical of the treatment of security researchers conducting human rights work.

Ola Bini's arrest and continuing detention have been protested by his peers working in the intersection of human rights and technology. (See https://freeolabini.org/en/statement/).

What are the main advances and strengths concerning the protection and promotion of

the work of human rights defenders in your country or in the region? What are the main setbacks and obstacles/challenges?

Within the context of protecting human rights defenders who use, or contribute to the development of rights-protecting technology in the course of their work, the principle strength is a network of supported and supportive technologists who collectively share their resources publicly. This kind of work is being used in a decentralized way by human rights defenders around the world.

The greatest challenge is the use of criminal law as a response to socially beneficial behavior by technologists who work to protect the right to privacy in the digital age. These cybercrime laws use ill-defined terms, and fail to narrowly tailor the punishable offense. They fail to meet the requirements of the Legality Principle as established by the Inter-American Human Rights Standards, which prescribes that any restriction of a right through the use of criminal law must be prescribed by law. Vague and ambiguous criminal laws are an impermissible basis to restrict the rights of a person.

Additionally, these criminal provisions fails to clarify the definition of *malicious intent* or *mens rea*, and actual damage turning general behaviors into strict liability crimes. These cybercrime laws can have deleterious effects on free expression of security researchers since they can be interpreted broadly by prosecutors seeking to target individuals.

See for example, Article 232 of the Ecuadorian Criminal Code (excerpted below): a provision that fails to meet the Legality Principle requirement, fails to make clear malicious intent, and lacks specificity, leading to the vague re-definitions of crimes, beyond the original intent of the legislators.

In contrast, for example, in some cybercrime provisions the *intent* requirement is more clearly present in the way cyber-offenses are worded. Act 19.223 of Chile, for instance, punishes illicit access but establishes that, in order to be punishable, the action must be deployed with the intent (*desire*) of unlawfully getting, using, or learning information that is contained within a given information system. This subjective element safeguards the actions of technologists who might access systems with no permission but with no intention of causing harm. The same is established by Article 3 of Chile's act, which demands maliciousness to punish those who affect the integrity of data. For more examples of criminal legislations, please read "Protecting Security Researchers' Rights in the Americas", https://www.eff.org/coders-rights-americas .

What should be changed in your country or region to contribute to a safe and conducive environment for the defence of human rights?

Prosecutions of technologists working in this space should be treated in the same way as the prosecution of journalists, lawyers, and other human rights defenders — with extreme caution and with regard to the risk of politicization and misuse of such prosecutions.

States should ensure criminal law provisions that affects technologists are prescribed by law, and are clear and precise. Those laws should also include a clear requirement of malicious intent. Without a malicious intent requirement, any criminal law provisions can harshly criminalize "breaking security," potentially without any requirement for harm or damage, and seemingly without regard to whether the purpose was beneficial. Such legislation can have detrimental chilling effects on technologists' free expression rights. Finally, judges should understand that laws that fail to specify the need for volition or malicious intent to constitute a crime nevertheless still permit judges, applying general principles of law, to determine that without damage, there is no crime. (See "Protecting Security Researchers' Rights in the Americas", "Judges and Interpretations", https://www.eff.org/wp/protecting-security-researchers-rights-americas#criminal_intent_security_research , and the Sorianello case below.)

- **Defenders most at risk:**

What are the groups or sectors of human rights defenders most at risk? Please explain the distinct nature of the risks and threats faced by women human rights defenders, indigenous peoples, Afro-descendants and other groups.

N/A

Concerning groups or sectors of human rights defenders in a situation of greater risk, do you see any change since 2016?

We are concerned that the pattern of the politicized targeting of technologists is beginning to emerge as a trend across the region, as it has done within the United States, and beyond the Americas.

To give two other examples other than that of Mr Bini:

In mid-2015, the computer crime division of the Buenos Aires metropolitan police raided the home of a researcher, Joaquín Sorianello, who had reported serious vulnerabilities in the electronic voting system selected for that city's elections to the manufacturers of the machines. Rather than being supported for his warning, a local judge signed an order censoring news of the vulnerabilities. https://www.eff.org/deeplinks/2015/07/buenos-aires-censors-and-raids-technologists-fixing-its-flawed-e-voting-system

In 2018, the Canadian police threatened to prosecute another researcher, for writing and using an automated script to download public records from a government website. While the charges were later dropped, the chilling effects on other technologists exercising their right of access to information from the state is clear. (See https://www.eff.org/deeplinks/2018/04/dear-canada-accessing-publicly-available-information-internet-not-crime)

What are the main protection concerns and challenges faced by human rights defenders when carrying out activities in both the public and private spheres, including through digital means?

As we have stated, we believe that broad cybercrime laws, and their misuse by political actors, can directly challenge human rights defenders.

- **Attacks or restrictions:**

What are the most recent statistics on attacks and restrictions against human rights defenders in the country or region? Please indicate the source of the information and indicate the period covered.

N/A

What are the main types of attacks and restrictions against human rights defenders in the country or region? Do you see any change since 2016? If possible, identify if there is a geographic area that needs to be highlighted in particular.

N/A

Could you identify one or more patterns in the type of aggressors/perpetrators? Are these state or non-state actors?

These attacks comes from state actors who see the legitimate work of a technologist as a security threat.

What are the consequences and impact of the attacks and restrictions at the individual and collective level (both in the scope of the organizational space and in broader social spaces)?

- Can create a cascade of self-censorship that inhibits other technologists working to protect and secure our critical infrastructure.
- Contributes to an atmosphere that categorises information security work as dangerous and anti-social, even though this work is vital for the protection of privacy in the digital age.

What types of attacks do you consider to particularly affect women human rights defenders (in urban and rural areas, members of indigenous and Afro-descendant communities, and other groups)?

N/A

- **Guarantees for the free exercise of the defense of human rights:**

Do you consider there is any aspect of the normative, institutional and public policy framework that promotes or hinders the free exercise of the defense of human rights?

As previously noted, the treatment of cybercrime law as being separate and unconnected to human rights considerations is an ever-present concern.

For its effect within North, Central, and South America, see our report "Protecting Security Researchers' Rights in the Americas", https://www.eff.org/coders-rights-americas .

It is also significant that, even poorly-drafted cybercrime laws outside the region can have am effect on local activists. For instance, Pakistan's wide-ranging Prevention of Electronic Crimes Bill (PECB), passed in 2016, claims jurisdiction over "every citizen of Pakistan *wherever he may be",* and "appl[ies] to *any act committed outside Pakistan* by any person if the act constitutes an offence under this Act and affects a person, property, information system or data location in Pakistan." (See *https://www.eff.org/deeplinks/2016/08/global-ambitions-pakistans-new-cyber-crime-act*).

Have you identified as an existing problem in your country or in the region the misuse of criminal law to criminalize human rights defenders for their activity? If so, please indicate in which contexts it occur, which actors are involved, and what would be the main causes or the factors that generate it.

Overbroad cybercrime laws are generated by a failure to incorporate human rights considerations into the drafting and application of laws regarding technology; their misapplication against human rights defenders by states is caused by the increasing use of digital technology by human rights defenders, and the increasing important of providing secure, independent technology to human rights defenders.

If relevant, under what crimes are human rights defenders wrongly accused? If possible, provide concrete examples.

To use our flagship case, Ola Bini is currently being charged with Article 232 of the Ecuadorian Criminal Code:

> Any person who destroys, damages, erases, deteriorates, alters, suspends, blocks, causes malfunctions, unwanted behaviour or deletes computer data, e-mails, information processing systems, telematics or telecommunications from all or parts of its governing logical components shall be liable to a term of imprisonment of three to five years, or:
>
> Designs, develops, programs, acquires, sends, introduces, executes, sells or distributes in any way, devices or malicious computer programs or programs destined to cause the effects indicated in the first paragraph of this article, or:
>
> Destroys or alters, without the authorization of its owner, the technological infrastructure necessary for the transmission, reception or processing of information in general.

If the offence is committed on computer goods intended for the provision of a public service or linked to public safety, the penalty shall be five to seven years' deprivation of liberty.

This highlights two consistent problems with cybercrime laws: the statute can be interpreted in such a way that any software that could be *potentially* misused creates criminal liability for its creator; indeed, potentially more liability than those who conduct malicious acts. It also, in an online environment where authorization is generally implicitly assumed rather than explicitly agreed, can be read to require authorization for any legal action.

This allows misguided prosecutions against human rights defenders to proceed on the basis that the code created by technologists *might possibly* be used for malicious purposes; and that because an individual has not gained prior explicit authorization for any given service, they must be in violation of the law.

- **Access to justice and reparation:**

Could you provide information on the state of investigations of crimes committed against human rights defenders?

We refer the commissioners to the legal team defending Ola Bini's case, who are contactable via https://freeolabini.org/ .

What measures has the State taken to guarantee adequate reparation and guarantees of non-repetition? Please refer to concrete examples.

N/A

- **Preventive and reactive actions concerning attacks against human rights defenders:**

What measures, legislation, policies and mechanisms have had a positive or negative impact on generating safe contexts for human rights defenders? Do you know cases that could illustrate this?

N/A

If relevant, please include an assessment of national mechanisms for the protection of human rights defenders. What has been their real scope and effectiveness? Please indicate the reasons for this assessment.

N/A

Thank you for your participation in this questionnaire!

Please attach any documents that might be relevant and useful to the report (e.g., reports, flagship cases). You can send them by e-mail to adesouza@ohchr.org as well as any questions or observations to this questionnaire.