June 28, 2021

Secretariat of Human Rights of the Republic of Ecuador

Ms. Bernarda Ordóñez Moscoso
Secretary of Human Rights.

Mr. Felipe Ochoa
Deputy Secretary of Human Rights

We respectfully address the Secretariat of Human Rights for the purpose of **presenting concerns on the prosecution of the computer security expert Mr. Ola Bini in Ecuador** – a case of great interest to the remit of the Human Rights Secretariat given the due process and other rights violations involved. *This communication is particularly relevant given the resumption of Mr. Ola Bini's pre-trial hearing **on June 29**, which should receive the Secretariat's special attention*. The Human Rights Secretariat seems also rightfully positioned to examine the irregularities and violations surrounding Mr. Bini's case.

The Electronic Frontier Foundation (EFF) is an international non-profit civil society organization defending human rights in the digital world.[1] Founded in 1990, EFF champions users' human rights through impact litigation, policy analysis, grassroots activism, and technology development. EFF's mission is to ensure that technology supports human rights for all people of the world. EFF has over 30,000 supporters in 99 countries around the globe.

Mr. Bini's case has profound implications for, and sits at the center of, the application of human rights and due process, a landmark case in the context of arbitrarily applying overbroad criminal laws to security experts. Mr. Bini's case represents a unique opportunity for the Human Rights Secretariat Cabinet to consider and guard the rights of

[1] See more of our work at <https://www.eff.org>.

security experts in the digital age. Security experts protect the computers upon which we all depend and protect the people who have integrated electronic devices into their daily lives, such as human rights defenders, journalists, activists, dissidents, among many others. To conduct security research, we need to protect the security experts, and ensure they have the tools to do their work.

Since our founding in 1990, EFF has been concerned with the use of cybercrime law to target technologists engaged in cutting-edge exploration of technology, where all too often beneficial security research is mistaken for bad behavior. We have opposed in the courts the prosecution or intimidation of technologists, particularly digital security experts, and stepped in to defend security researchers from misunderstandings made by law enforcement. [2]

Due to the relevance of this emerging cybercrime case in Latin America, from July 29th to August 2nd, 2019, EFF conducted an on-site visit to Ecuador to investigate complaints of injustice related to Mr. Bini's case, and continued monitoring his legal prosecution in the years since.

Below you will find the main points we would like to bring to the Secretariat's attention as a contribution for your office's further examination of the matter. First, we explain how the work of security experts is crucial in ensuring everyone's rights and security. Second, we discuss how Mr. Bini's life's work is consistent with improving people's protection in the daily use of technology. Third, we raise EFF's concerns regarding Mr. Bini's prosecution, such as due process and other rights violations, the weak case against the security expert considering publicly available evidence, and the troubling political framing surrounding the case.

We believe the Human Rights Secretariat can play a relevant role by bridging the protection of security experts to the broader mission of upholding human rights.

[2] See more at <https://www.eff.org/issues/coders>.

The work of security experts is vital to safeguard everyone's rights and security

By identifying and disclosing software and hardware vulnerabilities, security experts improve security for every user who depends on information systems for their daily life and work. However, all too often, they are threatened with laws intended to prevent malicious intrusion, even when their own work is anything but malicious. Digital communication technology and privacy-protective tools like end-to-end encryption have made the work of journalists, lawyers and human rights defenders safer against cyber-criminals and the harassment of repressive regimes. Unfortunately, these impressive gains in privacy and security have put the technologists building those tools on the spot and increasingly subject them to the same harassment.

EFF explained the perils of overbroad cybercrime laws, and the threats of their overbroad interpretation by law enforcement authorities, in our 2018 paper *Protecting Security Researchers' Rights in the Americas*.[3] The paper draws on rights recognized by the American Convention on Human Rights, and examples from North and South American jurisprudence, to analyze how these fundamental human rights apply to security researchers and how we might best interpret human rights safeguards to protect the digital security work that is increasingly vital to ensure our rights and safety in the day-to-day use of technology.

Based on our legal analysis of criminal laws, the paper reflects concerns about the potential to spread harassment and prosecutions of security experts building secure software in the Americas.[4] Many cybercrime provisions that fail to clarify the definition of malicious intent and actual damage can turn the general work of security experts into strict liability crimes. Our paper recommends that both intent and actual damage should be part of the definition of criminal liability in cybercrime laws. Without these elements the law can burden the fundamental right to free expression and the socially beneficial work of security researchers, allowing provisions to be interpreted broadly to unjustly target

[3] See more at <https://www.eff.org/coders-rights-americas>.
[4] EFF has reported about some of those cases: *Buenos Aires Censors and Raids the Technologists Fixing Its Flawed E-Voting System*(<https://www.eff.org/pt-br/node/86903>); *Dear Canada: Accessing Publicly Available Information on the Internet Is Not a Crime* (<https://www.eff.org/pt-br/deeplinks/2018/04/dear-canada-accessing-publicly-available-information-internet-not-crime>); *With a Raid on Javier Smaldone, Argentinian Authorities Have Restarted Their Harassment of E-Voting Critics* (<https://www.eff.org/pt-br/deeplinks/2019/11/raid-javier-smaldone-argentinian-authorities-have-restarted-their-harassment-e>).

individuals. Such laws can be easily abused to harass security researchers who are committed to protect the public interest.

The prosecution and detention of the Swedish-born open-source developer, Mr. Ola Bini, in Ecuador in April 2019 illustrates the growing seriousness of this issue in Latin America.

Background of security expert Mr. Ola Bini

Mr. Bini is known globally as a computer security expert and an advocate for a secure and open Internet. Mr. Bini is primarily known for his non-profit work on the secure communication protocol, OTP, and contributions to the Java implementation of the Ruby programming language. He contributed to the European Union's DECODE Project, [5] an initiative aimed at providing tools to put people in control of their data. He has also contributed to EFF's Certbot project, [6] which provides easy-to-use security for millions of websites around the world. He moved to Ecuador during his employment at the global consultancy ThoughtWorks, which has an office in Quito, later co-founding a non-profit organization devoted to creating user-friendly security tools (the *Centro de Autonomía Digital*).[7]

As this brief description shows, **Mr. Ola Bini's global reputation in the information security community is mainly as a "builder" of secure software**. He **is not known as the particular kind of security researcher who tests flaws in software or services trying to "intrude" in them**. Although there is nothing wrong with testing and finding flaws in security, Mr. Bini is well known for his defensive work: making sure privacy tools are designed so that others cannot break into them. Therefore, his detention and investigation for "assaulting the integrity of computer systems" in April 2019 was puzzling and made little sense. The circumstances of his detention were equally puzzling.

[5] See more at <https://decodeproject.eu/>. DECODE Project provides tools that put individuals in control of whether they keep their personal information private or share it for the public good.
[6] Certbot is a free, open-source software tool for automatically using *Let's Encrypt* certificates, which give people the digital certificates they need in order to enable HTTPS security for websites, for free. Let's Encrypt is a free nonprofit certificate authority, which has grown to become the world's largest certificate authority. The security of the modern web depends on HTTPS and the certificate authorities that support HTTPS. See more at <https://certbot.eff.org/about/>.
[7] See more at <https://autonomia.digital/>.

Mr. Ola Bini's Detention

Mr. Ola Bini's April 2019 arrest was preceded by a press conference hours after the government had ejected Julian Assange from Ecuador's London Embassy, and was 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 were supposedly involved in trying to establish an alleged piracy center in Ecuador, including two Russian hackers, a Wikileaks collaborator, and a person close to Julian Assange. [8] However, no evidence to back those claims was provided.

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 on programming that any programmer might have and common computer devices, such as USB sticks and security keys, that had been confiscated from Mr. Bini's home and his person. [9]

From our experience working with the information security community for over 30 years, digital security experts across the globe often have habits and behavior that outsiders can find eccentric or suspicious. Since security researchers study the privacy and security risks associated with emerging technologies, they tend to collect technical hardware, encrypt all of their communications and lock down their computers. Those who build security software will be most conscious of their privacy and security, like someone who works with COVID-19 patients will be more conscious on how to protect themselves against the virus. Owning such devices and preserving the security of one's communications and equipment are not a crime, but they can make those unacquainted to this community think there is something wrong.

[8] See more at <https://www.eluniverso.com/noticias/2019/04/11/nota/7279946/jackers-rusos-miembro-wikileaks-viven-ecuador-denuncia-maria-paula/>.
[9] See at: <https://www.planv.com.ec/historias/politica/ola-bini-el-agente-wikileaks> (our translation).

EFF's monitoring of Mr. Bini's case

Visit to Quito and our conclusions on the political nature of Mr. Bini's prosecution

In July 2019, EFF carried out an on-site visit in Quito to investigate our concerns that Ecuador's authorities kept prosecuting the legal case against Mr. Bini without details about the digital attack, or about what had been hacked, in addition to the initial irregularities of the case.

In our trip, EFF spoke to journalists, politicians, lawyers, and academics, along with Mr. Bini and his defense team. We learned more about the *Habeas Corpus* ruling that released Mr. Bini after 70 days of imprisonment, which has qualified his detention as illegal and arbitrary. By then, Mr. Bini's lawyers told us they had counted more than 60 violations of due process in the trial.[10] Journalists have reiterated the lack of evidence against Mr. Bini since no-one could give them concrete descriptions of what the security expert had done.

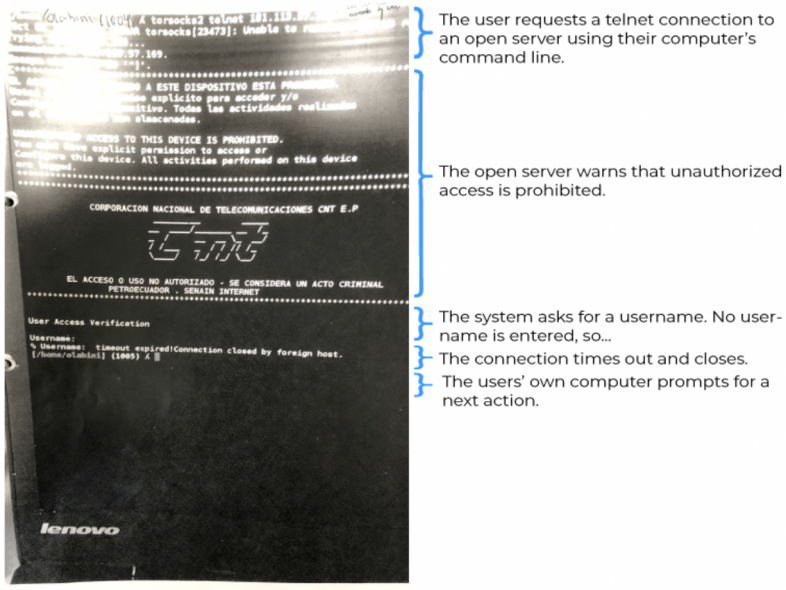
We held a press conference at the end of our visit to Quito, where we concluded that Mr. Bini's prosecution represented "a political case, not a criminal one." [11] An important factor affecting the status of the trial was the perceived political consequences of either abandoning the case, or continuing to prosecute. The details of who is responsible, or who stood to benefit from Mr. Bini's prosecution, varied depending on who we spoke to. However, we were disturbed by how much the political effect of Mr. Bini's innocence or guilt appeared to be affecting the investigation. Based on the interviews and circumstances of the case, **we emphasized that Mr. Bini's innocence or guilt is a fact that should be determined by a fair trial that follows due process, separate from its political ramifications**.

[10] See at <https://twitter.com/calilo84/status/1152257124040368130>. As for Ola Bini's detention, his defense has detailed a number of irregularities in a press release <https://goatsing.wordpress.com/2019/04/13/press-release-on-the-detention-of-ola-bini-2/>.
[11] See at <https://www.eff.org/deeplinks/2019/08/ecuador-political-actors-must-step-away-ola-binis-case>.

The publicly available evidence shows a weak case against Mr. Bini, based on misunderstandings of technology

On August 16, 2019, right after our mission to Ecuador, local news media released a photo that was used to support an allegation that Mr. Bini illegally entered a router of the National Telecommunications Corporation (CNT), information that was later used in Mr. Bini's pre-trial hearing.

The photo was a screenshot, shown below, said to be taken from Mr. Bini's mobile phone. The press reported that the phone was unlocked by police after seized security footage revealed Mr. Ola Bini's PIN when he used his phone in his own office elevator: "The camera captured the moment when the computer scientist approached the elevator and typed the eight-digit code on the screen of his cell phone." [12] This evidence was not the proof alleged by the prosecutors. As EFF explained in an August 23, 2019 report,[13] the screenshot was, instead, consistent with someone who checked a publicly accessible server and **obeyed** the servers' warnings about usage and access. The screenshot (with our annotations):



[12] See, for example, the following news article: <https://www.elcomercio.com/actualidad/ola-bini-fiscalia-celular-cnt.html> (our translation).
[13] See at <https://www.eff.org/deeplinks/2019/08/telnet-not-crime-unconvincing-prosecution-screenshot-leaked-ola-bini-case>.

As EFF's technologists explained, those knowledgeable about the Unix-style command line shells and utilities shown in the photo would easily recognize it as the photograph of a laptop screen, showing a "telnet session," an insecure communication protocol that has largely been abandoned for public-facing technologies). Our technology team explained:

> "Command line interactions generally flow down the page chronologically, from top to bottom, including both textual commands typed by the user, and the responses from the programs the user runs. The image shows, in order, someone – (presumably Bini, given that his local computer prompt shows "/home/olabini") – requesting a connection, via Tor, to an open telnet service run on a remote computer.
>
> Telnet is a text-only communication system, and the local program echoes the remote service's warning against unauthorized access. The remote service then asks for a username as authorization. The connection is then closed by the remote system with a 'timeout' error, because the person connecting has not responded.
>
> The last line on the screen capture shows the telnet program exiting, and returning the user to their own computers' command line prompt."

We concluded that **the screenshot itself was not demonstrative of anything beyond the normal procedures that computer security professionals conduct as part of their work**:

> "A user discovers an open telnet service, and connects to it out of curiosity or concern. The remote machine responds with a message by the owner of the device, with a warning not to log on without authorization. The user chooses to respect the warning and not proceed."

The media also leaked a portion of a conversation between Mr. Bini and his system administrator, Ricardo Arguello, a well-known figure in the Ecuadorian networking and free software communities. Although the entire conversation was not released, the above image and our analysis can also explain the fraction of the following excerpt where Mr.

Bini sent the above screenshot, to which Arguello replied, “It’s a router. I’ll talk to my contact at CNT.”

As our technology team explained, if someone found a service that was insecurely open to telnet access on the wider Internet, that’s what you might reasonably and responsibly do — send a message to someone who might be able to inform the service’s owner, with evidence that their system is open to anyone to connect. And under those conditions, Arguello’s response is just what a colleague might say back — that they would get in touch with someone who might be able to take the potentially insecure telnet service offline, or put it behind a firewall.

Using Tor is not a crime

According to Mr. Bini’s report of the pre-trial hearing, the CNT lawyer unfairly relied on use of Tor, a common internet security tool, as an indication of illegal behavior.[14] The *El Comercio* reporter, Valentín Díaz, understood these concerns, saying "What a danger! Journalists, activists, lawyers, engineers and people who generally store sensitive data use @torproject. It's not that we want to commit illegalities. It's the responsible thing to do. I can't surf everywhere exposing my identity and - incidentally - that of my contacts."[15]

Using the Tor tool to access and browse the internet is not a crime, nor should it be considered a suspicious behavior. Tor is an open-source, volunteer-run browser that relies on strong encryption to provide robust privacy protections in online browsing and communications. [16] Originally deployed in the U.S. for the primary purpose of protecting Navy communications, it is currently used by journalists, human rights activists, military, law enforcement officers, IT professionals, bloggers, and others.[17] By protecting users’ identities and locations, Tor offers a crucial protection to journalists and their sources, to witnesses facing harassment, and to human rights defenders and political dissidents threatened in their lives or physical safety, among others. It is also commonly used to protect against commercial tracking and other more mundane invasions of privacy all too

[14] See Mr. Ola Bini's post at: <https://twitter.com/olabini/status/1339689974275432454>.
[15] See at: <https://twitter.com/v4li3nte/status/1339758702904176640> (our translation).
[16] See more at <https://www.torproject.org>.
[17] See at <https://2019.www.torproject.org/about/torusers.html.en>.

common online. Those who build secure software also commonly use Tor, because they know the tool will secure their communications.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has stressed that:

> "Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality."[18]

Recent developments of Mr. Ola Bini's case

More recently, in April 2021, the Judge partially granted Mr. Bini's *Habeas Data* recourse, originally filed in October 2020 against the National Police, the Ministry of Government, and the Strategic Intelligence Center (CIES). The decision has determined that the CIES had to provide information related to whether the agency has carried out surveillance activities against the security expert. **The ruling deemed that CIES unduly denied such information to Mr. Bini, failing to offer a timely response to his previous information request**.[19]

[18] See the *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (A/HRC/29/32), paragraph 12. See at: <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32>.
[19] See more at: <https://ecuadortoday.media/2021/04/29/victoria-parcial-para-ola-bini-juez-reconocio-infraccion-del-cies-al-negar-entrega-de-informacion/>.

In the criminal case, **the pre-trial hearing is set to resume its examination on June 29th**, more than two years after Mr. Bini was arrested. The hearing was most recently suspended in December 2020.

The repeated suspensions and resumptions of the pre-trial hearing raises human rights concerns that also should be examined by the Secretariat. The Office of the IACHR Special Rapporteur for Freedom of Expression expressed concern with the fact that Mr. Ola Bini's trial continued to be held in abeyance during 2020. As the Special Rapporteur 2020's annual report points out, pre-trial hearings were suspended and rescheduled at least five times during that year. [20] Since Mr. Bini's arrest in April 2019, the alleged charges and evidence against him still wait for a proper assessment by the court, and Mr. Bini, as a suspect under trial, continues to be deprived of the full enjoyment of his rights.

International reverberations and Ecuador's Human Rights Secretariat

The IACHR report and EFF's monitoring of the case illustrate the **international resonance of Mr. Ola Bini's prosecution**. The controversies and irregularities around this case, some of them highlighted in this letter, have made the case part of the discussion in different international venues devoted to the protection of human rights in its intersection with technology (e.g. Internet Governance Forum, Latin American Internet Governance Forum, RightsCon) [21] as well as triggered statements of human rights bodies, such as the UN, [22] and human rights entities, such as Amnesty International.[23] Human and digital rights groups, such as APC, Article 19, Derechos Digitales, Access Now, Fundación Karisma, have been also closely monitoring the developments of the case.

Ecuador's new administration, through the Secretariat of Human Rights, has a key opportunity to assess and address the complaints of rights violations in Mr. Bini's prosecution. During our visit to Quito in 2019, we sought to present our concerns regarding the case by extending our meeting invitations to the General Public Prosecutor

[20] See at <http://www.oas.org/es/cidh/docs/anual/2020/capitulos/rele.PDF>, paragraph 545.
[21] See, in order, at: <https://www.accessnow.org/join-our-statement-for-the-protection-of-digital-rights-defenders/>; <https://www.eff.org/pt-br/deeplinks/2019/08/eff-se-suma-organizaciones-de-america-latina-que-se-oponen-la-acusacion-de-ola>; and <https://rightscon2019.sched.com/event/QX9W/the-imprisonment-of-ola-bini-building-solidarity-and-protecting-the-community>.
[22] See at: <https://freeolabini.org/es/LetterUN/>.
[23] See at: <https://www.amnesty.org/es/documents/amr28/0871/2019/es/>.

and the Minister of Interior, but we haven't obtained a response. We welcome the Human Rights Secretary's declarations that the body will look into complaints of rights violations committed in the country.[24] The Secretariat is rightfully positioned to examine the irregularities and human rights violations surrounding Mr. Bini's case, as well as to follow the developments in his prosecution and monitor that the security expert can receive a proper and fair trial.

Conclusion

This letter brings to the Secretariat's attention EFF's concerns with Mr. Bini's prosecution based on our longstanding work countering the unfair criminal persecution of security experts. We point out due process and other rights violations already acknowledged in judicial decisions, the flimsy case against Mr. Bini considering publicly available evidence, the unsettling pattern of pre-trial hearings' rescheduling or suspension, and the need to ensure Mr. Bini a fair trial divorced from the politicized framing that has surrounded his prosecution from the start.

The Human Rights Secretariat is well positioned to examine the irregularities and violations related to Mr. Bini's case, and we respectfully urge the Secretariat to assess and address such complaints of injustice, as well as to guard that Mr. Bini can receive a fair trial. We thank you in advance for your thoughtful consideration, remaining at the Secretariat's disposal for any clarifications.

[24] See at: <https://www.facebook.com/LaPostaEc/videos/781619866053286>.