Written Submission for the Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR/RFOE)

Public Consultation on:

Digital Surveillance Technologies and Human Rights

2024

Submitted by the Electronic Frontier Foundation
(Veridiana Alimonti, Katitza Rodriguez, David Greene, and George Wong)

Introduction

We thank you for the opportunity to provide comments in response to the Consultation Questionnaire for the preparation of a thematic report on digital surveillance technologies and human rights. The Electronic Frontier Foundation (EFF) is an international non-governmental organization dedicated to protecting civil liberties and human rights in the digital world through impact litigation, policy analysis, grassroots activism, and technology development. EFF has been active since 1990, engaging directly with digital users worldwide and providing leadership on cutting-edge issues of free expression, privacy, and related human rights.

Our submission builds on EFF's steady work monitoring and analyzing government digital surveillance and its impacts in individuals and communities. Particularly, it draws on the Necessary and Proportionate Principles on the Application of Human Rights to Communications Surveillance (Necessary & Proportionate principles) and comparative analysis of privacy legal frameworks vis-à-vis international human rights law.

Our submission focuses on Latin American countries and related regulatory gaps, concerning trends, and best practices. In mapping those, it also takes into account almost a decade of the project *¿Quién Defiende Tus Datos?*, which have assessed Internet Service Providers' privacy policies and practices in eight Latin American countries and Spain, flagging transparency and accountability limitations also related to problematic legislation and government demands. Our responses address questions in sections (1), (2) and (5) of the Consultation Questionnaire.

Building on this analysis, the finalization of the UN Cybercrime Convention has raised additional concerns about the expansion of international cooperation in surveillance. The treaty introduces broad provisions for cross-border access and police data sharing powers, which lacks sufficient robust privacy and data protection safeguards. This is particularly concerning for Latin America, where oversight mechanisms are often weak, and human rights standards fall. Additionally, the Convention's authorization of predictive policing and biometric databases heightens the risk of discriminatory impacts and inadequate protection of sensitive data, posing serious threats to human rights in the region.

Regarding our litigation work in the U.S., EFF has been at the forefront of challenging the legality of U.S. mass surveillance programs implemented following the 9-11 terrorist attacks. EFF filed and litigated three lawsuits over the course of 16 years, but U.S. courts were never able to consider the merits of the claims. EFF has also been active in advocacy regarding the legislative renewals and revisions of the surveillance programs. We should also highlight that EFF has done extensive analysis on Street-Level Surveillance (particularly in the U.S.) and Border Surveillance Technologies (especially in the US-México border).

Although this submission does not address these lawsuits and resources, our team can provide further information in case the Office of the Special Rapporteur is interested in delving deeper into these topics.

Comments Based on the Consultation Questionnaire

1. Incidents of misuse

Unfortunately, incidents of misuse of digital surveillance technologies by state authorities in Latin America are a persistent issue in the region. State arbitrary surveillance practices target journalists, human rights defenders, community leaders, environmental advocates, political dissidents, politicians, and judges, among others, who may disturb or seem a threat to state authorities with the means and opportunity to unleash surveillance actions.

On the upside, many organizations and advocates have fiercely documented, exposed, and fought against illegitimate state surveillance, also providing support for the victims. The first major challenge lies precisely in the victims and the larger society becoming aware of these practices. We touch upon this and other challenges in the following sections of our submission. In this section, we provide further information about a specific case—the unlawful and arbitrary monitoring of political figures, journalists, and public servants by the Brazilian Intelligence Agency (ABIN) by using the software *First Mile*, among other tools.

First Mile and ABIN's Unlawful "Clandestine" Monitoring

First revealed in March 2023, the unlawful use of location tracking software by intelligence forces in Brazil has hit the headlines repeatedly and sparked important investigations. The newspaper *O Globo* uncovered that during former president Jair Bolsonaro's administration, ABIN officials used the software *First Mile*, from the Israeli company Cognyte, without any official protocol. Investigations conducted by the Brazilian Federal Police later established that these officials "acted under the command" of the then director of ABIN as part of a parallel surveillance structure within the intelligence agency. In a related ruling, the Supreme Court Justice Alexandre de Moraes stated that:

> "The use of the FIRST MILE system took place mainly during the tenure of police chief ALEXANDRE RAMAGEM, who held the position of DIRECTOR GENERAL from 07/09/2019 to 07/30/2022. The use of the FIRST MILE tool substantiated in the 60,734

> (sixty thousand, seven hundred and thirty-four) records identified in the “TARGET” table covers the period from 06/02/2019 to 27/04/2021." (par. 156; our translation)

First Mile was purchased under a bidding exemption ("dispensa de licitação") during former president Michel Temer's administration and has the capacity to monitor the steps of up to 10,000 cell phone owners every 12 months. *First Mile* can detect an individual based on the location of devices using mobile networks. By simply entering a person’s phone number, it's possible to check their position on a map. It also provides targets’ displacement records and "real-time alerts" of their movements. A high-ranking source at Abin told *O Globo* that the agency claimed using the tool for "state security" purposes, and on the grounds there was a “legal limbo” on the privacy protections for cell phone metadata.

The primary issue this case underscores is the lack of robust regulation and oversight of intelligence activities in Brazil. Second, while the Brazilian law indeed lacks strong explicit privacy protections for telephone metadata, the access to real-time location data enjoys a higher standard at least for criminal investigations (see section 2 (a) of this submission). Moreover, Brazil counts on key constitutional data privacy safeguards and case law that can provide a solid basis to challenge the arbitrary use of tools like *First Mile*.

News reports indicated and government authorities confirmed that the software exploits the *Signaling System n. 7* (SS7). As we explain in this article, SS7 is a set of telecommunication protocols that cellular network operators use to exchange information and route phone calls, text messages, and other communications between each other on 2G and 3G networks (4G and 5G networks instead use the Diameter signaling system, which also have issues). When a person travels outside their home network's coverage area (roaming), and uses their phone on a 2G or 3G network, SS7 plays a crucial role in registering the phone to the network and routing their communications to the right destination. We point out that the SS7 essential functions are prone to attacks:

> "SS7 identifies the country code, locates the specific cell tower that your phone is using, and facilitates the connection. This intricate process involves multiple networks and enables you to communicate across borders, making international roaming and text messages possible. But even if you don’t roam internationally, send SMS messages, or use legacy 2G/3G networks, you may still be vulnerable to SS7 attacks because most telecommunications providers are still connected to it to support international roaming, even if they have turned off their own 2G and 3G networks. SS7 was not built with any security protocols, such as authentication or encryption, and has been exploited by governments, cyber mercenaries, and criminals [...]. As a result, many network operators have placed firewalls in order to protect users. However, there are no mandates or security requirements placed on the operators, so there is no mechanism to ensure that the public is safe."[1]

[1] EFF recently filed a submission to the FCC on the security of SS7 and Diameter networks within the U.S. building on the comments of security experts about SS7 and Diameter exploits. The submission is available at https://www.fcc.gov/ecfs/document/10529224215816/1 .

Although the Brazilian case relates more specifically to location tracking, there are other common types of attacks exploiting SS7 vulnerabilities. A 2020's report commissioned by the Financial Inclusion Global Initiative (FIGI), which includes the International Telecommunications Union (ITU), lists eight common types of telecom attacks.[2]

Yet, according to a Federal Police's report, *First Mile* was only one of the tools used to carry out what the agency dubbed "clandestine actions". As the report explains:

> "The parallel structure carried out clandestine actions that ensured political advantages, [...], as well as economic advantages due to the strong indications of acts of passive corruption identified.
>
> The parallel structure therefore **used various systems** to carry out its clandestine actions. **Among the official systems, the FIRST MILE system** was used through the accesses of the military officer assigned to ABIN, GIANCARLO, who was a direct subordinate of federal police officer BORMEVET. **As for the clandestine systems, it has not yet been possible to identify its integrality**.
>
> [...]
>
> The FIRST MILE system, in fact, **was just one of the systems used** by the ORCRIM [criminal organization] and the senior managers were fully aware of its use." (par. 32-33 and 67; our translation and emphasis)

In Section 7.1 about clandestine actions against Justice Alexandre de Moraes, the report underlines—"The use of illegitimate systems, including those paid for in foreign currency (dollars and/or euros), is noteworthy in this specific case. There is no certainty as to which system paid for in dollars and/or euros was used [...] to monitor the Supreme Court Justice." (par. 193; our translation).

Having outlined the case and aspects of SS7 exploitation, we address some of the questions in the Consultation Questionnaire.

a. Targeted individual(s), community(ies), or entity(ies).

---

[2] The attacks are spam, spoofing, location tracking, subscriber fraud, interception, denial of service, infiltration attacks, routing attacks. FIGI. Security, Infrastructure and Trust Working Group. *Technical Report on SS7 vulnerabilities and mitigation measures for digital financial services transactions*. 2020, p. 11. Available at https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/Technical%20report%20on%20SS7%20vulnerabilities%20and%20mitigation%20measures%20for%20Digital%20Financial%20Services%20transactions.pdf See more about *Why SS7 Isn't Secure* in our article - https://www.eff.org/deeplinks/2024/07/eff-fcc-ss7-vulnerable-and-telecoms-must-acknowledge

The Federal Police's report describes a series of clandestine actions that ABIN officials carried out between 2019 and 2022. Section 5 of this report focuses specifically on people targeted by the software *First Mile*. The list of persons mentioned in section 5 can be found below:

- Jean Willys, journalist, activist and former Federal Deputy, and his family members;
- Rodrigo Maia, Federal Deputy and then President of the Chamber of Deputies;
- Joice Hasselmann, then Federal Deputy;
- Luiza Alves Bandeira, journalist at the Digital Forensic Research Lab (DFRLab);
- Pedro Cesar Batista, journalist;
- Hugo Ferreira Netto Loss, employee of the Brazilian Institute for the Environment and Renewable Natural Resources (Ibama)
- Roberto Cabral Borges, employee of Ibama.

According to the report, these events are only the minimal part of others still under analysis (par. 131).

Following sections of the Federal Police's report reveal other people targeted by clandestine and unlawful monitoring **without specifying the tools used**. Section 6 points out that ABIN officials' clandestine actions also targeted criminal investigations involving family members of former president Jair Bolsonaro. These are: (i) an investigation involving the former president's son Renan Bolsonaro; (ii) another involving the former president's son Flávio Bolsonaro; (iii) the investigation of Marielle Franco's murder;[3] (iv) the investigation of the case Adélio[4].

Section 8 of the report elaborates on the connection between monitoring activities and the production and dissemination of information and disinformation online to harm specific targets. **The report seems to use the term "clandestine actions" to refer to both surveillance and content dissemination-related activities**.[5]

[3] See more information at https://pt.wikipedia.org/wiki/Assassinato_de_Marielle_Franco
[4] See more information at https://oglobo.globo.com/politica/noticia/2024/06/11/pf-conclui-que-adelio-agiu-sozinho-em-atentado-contra-bolsonaro-em-2018.ghtml
[5] Regarding content production and dissemination activities aimed at harming opponents, the Federal Police report mentions other people involved beyond the "parallel structure" within ABIN. The report points also to two other hubs ("núcleos") dubbed "digital militias" and "Presidency of the Republic". The latter was formed by public officials in the presidential palace.

Based on the information provided in the report, we summarize below a list of mentioned targets of "'clandestine actions," including those we indicated above:[6]

JUDICIARY

- Alexandre de Moraes, Supreme Court Justice;
- Luis Roberto Barroso, Supreme Court Justice;
- Luiz Fux, Supreme Court Justice .

LEGISLATIVE

- Arthur Lira, current President of the Chamber of Deputies, and potentially his office staff;
- Rodrigo Maia, Federal Deputy and then President of the Chamber of Deputies;
- Potentially Marcelo Ramos, then Vice-President of the Chamber of Deputies;
- Kim Kataguiri, Federal Deputy, and his office staff;
- Joice Hasselmann, then Federal Deputy;
- Alessandro Vieira, Senator and member of the COVID-19 Parliamentary Inquiry Commission (CPI), which investigated the federal government;
- Omar Aziz, Senator and chair of the COVID-19 CPI;
- Renan Calheiros, Senator and rapporteur of the COVID-19 CPI, and potentially his office staff;
- Randolfe Rodrigues, Senator and vice-president of the COVID-19 CPI.

PEOPLE RELATED TO CRIMINAL INVESTIGATIONS INVOLVING BOLSONARO'S FAMILY MEMBERS

- All the main investigated people in the federal police investigation related to Renan Bolsonaro, including the businessman Luís Felipe Belmonte;
- Auditors of the Brazilian Federal Revenue related to an investigation against Flávio Bolsonaro: Christiano José Paes Leme Botelho, Cleber Homem da Silva, and José Pereira de Barros Neto;

[6] The list does not include people mentioned in the report that appear to have been solely the target of activities related to the production and dissemination of content and disinformation. They are: José Dirceu, politician (par. 242); Rodrigo Maria (par. 242); Marinho's family, related to the communications business group Globo (par. 242); Sérgio Moro, former judge and currently Senator (par. 242); Wilson Witzel, former Governor of Rio de Janeiro (par. 284 and 289), José Antonio Dias Toffoli, Supreme Court Justice (par. 287 and 289), and Geraldo Alckimin, currently Brazil's Vice-President (par. 289).

- Potentially Reinaldo Azevedo, a journalist, in connection with an investigation against Flávio Bolsonaro;
- The chief police officer in charge of the investigation of the murder of Marielle Franco and Anderson Gomes: Daniel Freitas da Rosa. Potentially, Simone Sibilo do Nascimento, public prosecutor.

OTHER PUBLIC SERVANTS

- Hugo Ferreira Netto Loss, employee of the Brazilian Institute for the Environment and Renewable Natural Resources (Ibama);
- Roberto Cabral Borges, employee of Ibama;
- Osvaldo Nico Gonçalves, chief police officer;
- Paulo Marino, then Director of the Federal Police.

JOURNALISTS, POLITICIANS, CIVIL SOCIETY, AND OTHERS

- Jean Willys, journalist, activist and former Federal Deputy, and his family members;
- João Doria, then Governor of São Paulo;
- Monica Bergamo, journalist;
- Vera Magalhães, journalist;
- Luiza Alves Bandeira, journalist at the Digital Forensic Research Lab (DFRLab);
- Pedro Cesar Batista, journalist;
- Sleeping Giants Brasil, an activist account on Twitter;
- Anna Livia Solon Arida, activist at Minha Sampa;
- Members of Instituto Sou da Paz;
- Staffers from Twitter Brazil;
- Fact-checking agencies "Aos Fatos" and "Lupa;"
- Potentially Lucas Azevedo Paulino, connected to Senator Alessandro Vieira.

As we don't have further details about other digital surveillance technologies employed in this case, the following responses will focus on the software *First Mile*.

b. Type of digital surveillance technology employed.
c. Identity of the surveillance technology operator, developer, middlemen, or other key state or private entities associated with the incident, if known.

The digital technology at issue is the location disclosure and tracking software *First Mile*. Please see more information about the surveillance capabilities of this software in our introduction to this section.

The surveillance operators using *First Mile* were those involved in ABIN's parallel surveillance structure. The Federal Police's report mentioned above (see also question *h*) details who are the members of this structure. The developer of the software *First Mile* is the company Cognyte. Specifically, the surveillance system was provided for the Brazilian government by the company Cognyte Brasil S.A.

d. Was legal, administrative, or other remedial action ever taken with respect to the incident? If so, what is the current status of the action?

A few action fronts are currently underway. We point out three in particular:

- **Investigation by the Federal Public Prosecution' Office:** The Federal Prosecutor's Office started to investigate the case in March 2023, right after the revelations by the Brazilian press and months before the Federal Police launched its own investigation operation. The Public Prosecutor's Office initiated this investigation following a complaint filed by the civil association Data Privacy Brazil. The investigation is underway.

- **Federal Police's investigation:** The Brazilian Federal Police launched "Operation Last Mile" in October 2023. In July 2024, the agency started the 4th phase of this operation. The police report we mention in our submission stems from such investigation.

- **Cases under the Brazilian Supreme Court:** In addition to the proceedings in which the Supreme Court has authorized Federal Police's investigative measures on ABIN's unlawful use of *First Mile* (PET 12.732), we should mention the constitutional challenge filed by the General Attorney's Office (initially ADO 84, turned into ADPF 1143). The constitutional challenge questions the lack of legal regulation of the use of malicious software by government bodies. The Supreme Court Justice in charge of the case, Cristiano Zanin, held a public hearing with experts about the secret use of digital monitoring technologies in June this year. The Justice has also requested information from Courts of Auditors across the country on government purchases of secret monitoring tools.

h. Links to any supporting documentation

We organize below links to supporting documentation:

Federal Police's report - https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2024/07/11115411/Pet-12732-representacao-policial-1.pdf

Justice Alexandre de Moraes' ruling in the PET 12.732 - https://www.conjur.com.br/wp-content/uploads/2024/07/decisao-moraes-abin-paralela.pdf

PET 12.732 - https://portal.stf.jus.br/processos/detalhe.asp?incidente=6971765

ADPF 1143 - https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814

Public hearings within ADPF 1143

June 10, 2024 I - https://www.youtube.com/watch?v=9ti7otML4_c

June 10, 2024 II - https://www.youtube.com/watch?v=JYBny5lr1A4

June 11, 2024 - https://www.youtube.com/watch?v=A0qfYU8eHfE

Links to related news reports can be found across the text of this section.

2. States' policies, laws, and regulations concerning use of digital surveillance technologies.

Drawing on the Necessary & Proportionate principles, EFF and partners have assessed national privacy legal frameworks to identify gaps and safeguards. The last iteration of this effort constitutes the series of reports "The State of Communication and Privacy Law" in Argentina, Brazil, Chile, Colombia, Mexico, Panama, Paraguay, and Peru. These reports provide a brief outline of legal standards for government lawful access to communications data in criminal investigations. As such standards are those often used to substantiate state digital surveillance, it's important to take them into consideration in identifying strengths and weaknesses of domestic legal frameworks. While this series of reports was published in 2020, most of the considered criteria remain without substantive changes.

(a) Competent Authorities and Related Legal Frameworks: Judicial Authorization Still Not a Rule for Disclosing Communications Data

The table below addresses the first two questions of section 2 based on our 2020 reports. The questions are:

a. Which state authorities are authorized to engage in digital surveillance activities, and pursuant to which specific laws and regulations?
b. Which if any laws or policies establish limits with regard to the nature, scope and duration of surveillance measures employed by state authorities; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged?

In some cases, the table content considers relevant updates that we also point out in the footnotes.

Table 1. Competent State Authorities to Access Communications Data in Criminal Investigations

	Interception of Communications	Access to Stored Content	Metadata
Argentina	Judicial authority, following a prosecutor's request.[7] **Emergency:** Direct request from prosecutors in the case of an ongoing crime of extortive kidnapping (pending judicial ratification within 24 hours).	Treated like interception	No specific regulation. Protected by the Constitution at the same level as "private papers," upon a judicial order (Halabi case).[8]

[7] See further information on the competent authority to conduct the interception of communications, under the authority of the Supreme Court and related controversies at "What's the legal authorization needed to access communications data?" in EFF's Argentina's 2020 report. We should note that references to Argentina's Criminal Procedure Code in EFF's 2020 report mainly relate to the *Código Procesal Penal Federal* (Decree 118/2019). Yet, the application of this Code in substitution for the *Código Procesal Penal* (Law 23.984) will take place gradually in the country. In the table of this submission, references to Argentina's Criminal Procedure Code consider Law 23.984 instead.

[8] in the Halabi case, the Supreme Court stated that case law referring to the inviolability of correspondence should apply to the context of interception of communications. The inviolability of correspondence should be authorized when: (i) there is a law determining the "cases" and "justifications" for which the content of such correspondence needs to be known; (ii) the basis of the law is the existence of a substantial or essential aim of the State; (iii) such restriction is compatible with the pursued legitimate aim; and (iv) the means to achieve it does not exceed what is strictly necessary. Halabi case, recital 25.

Brazil	Judicial authority, either *ex officio* or following the request of the public prosecutor or the police authority.	Upon judicial authorization.	**Online-related data:** upon judicial authorization. *Subscriber data as defined by legislation*: direct request from prosecutors or the Chief of the Civil Police is allowed in specific cases.[9] **Telephone-related data (fixed and mobile):** constitutional controversy on whether prosecutors and the Chief of the Civil police can directly access retained call records.[10] **Location data:** prior judicial order required for real-time access in specified legal cases (controversy on whether the judicial order requirement is lifted if the judge does not decide within 12 hours); the need for a prior judicial order is contentious for past/stored location data, but it should prevail due to constitutional safeguards.[11]
Chile	Judicial authority, following a prosecutor's request.[12]	Judicial authority, following a prosecutor's request.	**List of authorized ranges of IP addresses and of subscribers' IP numbers and connection logs:** prosecutor's request upon a judicial order.

[9] See further details at "Access to subscriber data" in the section "What's the legal authorization needed to access communications data?" in EFF's Brazil's 2020 report. Recently, the Supreme Court confirmed the validity of the provision in Brazil's Money Laundering Law (Art. 17-B, Law 9.613/1998) which allows the chief of the civil police and prosecutors to access subscriber information, as defined in the Decree 8.771/2016, without a previous judicial order. Read more at https://noticias.stf.jus.br/postsnoticias/norma-que-autoriza-mp-e-policia-a-requisitar-de-telefonicas-dados-cadastrais-de-investigados-e-valida-decide-stf/

[10] See "Access to retained traffic data" in the section "What's the legal authorization needed to access communications data?" in EFF's Brazil's 2020 report. See also InternetLab. O direito das investigações digitais no Brasil: fundamentos e marcos normativos, 2022 p. 42. https://internetlab.org.br/wp-content/uploads/2022/10/INTERNETLAB_O-DIREITO-DAS-INVESTIGACOES_PRINT_10-2022.pdf

[11] See "Location data" in the section "What's the legal authorization needed to access communications data?" in EFF's Brazil's 2020 report.

[12] Based on Chile's Criminal Procedure Code (*Código Procesal Penal*). This code began to be applied gradually in the different regions of the country between December 16, 2000 and June 16, 2005. The previous code (*Código de Procedimiento Penal*) remains in force for events that occurred before the entry into force of the new code.

Colombia	Attorney General's Office, through its judicial police authorities[13] (with subsequent judicial review).[14] **Emergency:** national government authority upon a judicial order.[15]	Attorney General's Office through judicial police authorities within the scope of their activities (with subsequent judicial review).	Attorney General's Office through judicial police authorities[16] within the scope of their activities.
México	Federal judicial authority, following the competent authority request.[17]	Treated like interception.	Judicial authority, following the competent authority request. **Emergency:** direct request from the Public Ministry (or the public servant to whom this power is delegated), with subsequent judicial review.[18]
Panamá	Judicial authority, following a prosecutor's request.[19]	Upon judicial authorization if considered "correspondence" or "private document." When not considered "electronic correspondence," prosecutors can access stored	**Stored data in seized devices not deemed "electronic correspondence":** prosecutors with subsequent judicial review.

[13] See more information at "Which authorities have the legal capacity to request access to communications data?" in EFF's Colombia's 2020 report. Telefónica's 2023 Transparency Report also provides updated information about competent authorities for the interception of communications in Colombia. https://www.telefonica.com/en/global-transparency-center/assistance-to-authorities/transparency-in-communications-report/

[14] See more information at "What's the legal authorization needed to access communications data?" in EFF's Colombia's 2020 report.

[15] See "Does the country have provisions about access to data in cases of emergency" in EFF's Colombia 2020 report.

[16] See more information at "What's the legal authorization needed to access communications data?" in EFF's Colombia's 2020 report. See updated list of such authorities at Telefónica's 2023 Transparency Report. Available at https://www.telefonica.com/en/global-transparency-center/assistance-to-authorities/transparency-in-communications-report/

[17] See more information at "What's the legal authorization needed to access communications data?" in EFF's México's 2020 report. We should note recent changes approved by the Mexican Congress that modify, among others, the powers granted to the country's National Guard. See more at https://comunicacionsocial.diputados.gob.mx/index.php/boletines/diputadas-y-diputados-aprueban-en-comision-incorporar-la-guardia-nacional-a-la-secretaria-de-la-defensa-nacional .

[18] See "Does the country have provisions about access to data in cases of emergency" in EFF's Mexico's 2020 report.

[19] We should note that the communications interception provision includes the authorization to the recording of conversations, interception of cyber communications, satellite tracking, and electronic surveillance. See more information at "What's the legal authorization needed to access communications data?" in EFF's Panamá's 2020 report.

		data in seized devices with only subsequent judicial review.	**Retained traffic data, subscriber data, and location data:** judicial authority or prosecutors' direct request with subsequent judicial review.
Paraguay	Judicial authority, following a prosecutor's request. The National Anti-Drug Secretariat can request a judicial order in cases involving the repression of drug trafficking.[20]	Upon judicial authorization.	Prosecutors can directly request metadata.
Peru	Judicial authority, following a prosecutor's request.[21]	Judicial authorization, following a prosecutor's request.	Upon judicial authorization, except for cases specified in Legislative Decree 1182. In those cases, the specialized police investigation unit can directly request from telecom operators access to real-time location data with only subsequent judicial review.[22]
Additional details on competent authorities		EFF's 2020 country reports also highlight legal provisions granting powers to access or request access to communications data by intelligence forces (like in Chile, México, and Paraguay); Parliamentary Committees of Inquiry (like in Brazil); and administrative authorities, like Brazil's *Receita Federal* and Chile's *Fiscal Nacional Económico*.	

Table 2. Laws and Regulations Considered (Criminal Investigations)

	Interception of Communications	[Complement] Access to Stored Content	Metadata

[20] See more information at "What's the legal authorization needed to access communications data?" in EFF's Paraguay's 2020 report.
[21] See more information regarding communications interception at "Which authorities have the legal capacity to request access to communications data" in EFF's Peru's 2020 report. We should note that the regulation of police access to cell phone or electronic device location data was amended in 2021.
[22] Law 31284 amended Legislative Decree 1182 in 2021. Before that change, LD 1182 limited this power to cases when a crime was in the process of being committed ("flagrante delicto" cases). Now it also covers preliminary investigations of a significant range of crimes, such as illegal mining and crimes against public administration.

Argentina	Articles 18 and 19, Argentinean Constitution. Supreme Court's Halabi Case (link). Articles 18-21 Law 19.798/1972, http://servicios.infoleg.gob.ar/infolegInternet/anexos/30000-34999/31922/texact.htm . Article 236, Criminal Procedural Code (*Ley 23.984*), https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/383/texact.htm .[23]	See also Articles 233-235, Criminal Procedural Code (*Ley 23.984*).	No specific regulation. Protected by the Constitution at the same level as "private papers," upon a judicial order (Halabi case).
Brazil	Article 5, X and XII, Brazilian Constitution. Article 3, Law 9.296/1996, http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm . Resolution 73/1998, under the terms of resolution 738/2020 of 12/21/2020, https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1495-resolucao-738 . Article 7, II, Law 12.965/2014 (*Marco Civil da Internet*), allowing the interception of online communications as per Law 9.296/1996, https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm	**Search and seizure:** Art. 240, Criminal Procedure Code, https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm . Related case law: STF, RE 418.416/SC, http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790 . STJ, HC 372.762-MG, https://stj.jusbrasil.com.br/jurisprudencia/511208828/habeas-corpus-hc-372762-mg-2016-0254030-1?ref=juris-tabs **Stored private online communications:** Article 7, III, Law 12.965/2014.	**Online-related data:** Articles 10, 13, and 15, Law 12.965/2014. *Subscriber information*: Art. 10 (3), Law 12.965/2014; Article 11, Decree 8.771/2016; Article 15, Law 12.850/2013; Article 17-B, Law 9.613/1998; Article 13-A, Criminal Procedure Code. **Telephone-related data (fixed and mobile):** Article 17, Law 12.850/2013. Article 22, National Telecommunications Agency's Resolution 426/2005 and Article 10, XXII, Resolution 477/2007. **Location data:** Article 13-B, Criminal Procedure Code for real-time access to location data. Case law exempting prior judicial order for stored location data related to telephone communications: STJ, HC 247.331-RS, https://www.jusbrasil.com.br/diarios/docu

[23] See *supra* note 7. The new *Código Procesal Penal Federal* regulates communications interception from Article 150 onwards. Available at https://www.argentina.gob.ar/normativa/nacional/decreto-118-2019-319681/texto .

			mentos/137159649/habeas-corpus-n-247331-rs-do-stj
Chile	Article 19 (5), Chilean Constitution. Articles 9 and 222, Law 19.696/2000 (Penal Procedure Code), https://www.leychile.cl/Navegar?idNorma=176595 . The procedure is regulated by the Decree 142/2005, https://www.leychile.cl/Navegar?idNorma=242261 . Article 14, Law 18.314/1984, https://www.bcn.cl/leychile/navegar?idNorma=29731 . Article 33 (a), Law 19.913/2003, https://www.bcn.cl/leychile/navegar?idNorma=219119 . Article 24, Law 20.000/2005, https://www.bcn.cl/leychile/navegar?idNorma=235507	See Articles 219-221, Penal Procedure Code.	Article 9, Penal Procedure Code (it requires prior judicial authorization to all proceedings that affect, deprive, or restrict the constitutional rights of the accused or a third party). **Retention and access to the list of authorized ranges of IP addresses and of subscribers' IP numbers and connection logs:** Article 222 (5), Penal Procedure Code. Article 6, Decree 142/2005.
Colombia	Article 15, Colombian Constitution. Article 200 and 235, Criminal Procedure Code, https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787 **Emergency:** Article 38 (e) of Act 137/1994 and related case law, https://www.corteconstitucional.gov.co/relatoria/1994/C-179-94.htm .	Articles 236 and 237, Criminal Procedure Code.	Interception-related rules. Regarding judicial police authorities, see Articles 200-205 Criminal Procedure Code. See also Articles 4 and 5 Decree 1704/2012 and the 2016 ruling of the Colombian Council of State, https://www.suin-juriscol.gov.co/clp/contenidos.dll/ConsejoEstado/30033603?fn=document-frame.htm$f=templates$3.0
Mexico	Article 16, Mexican Constitution. Articles 291 to 302, National Code for Criminal Procedure, https://mexico.justia.com/federales/codigos/codigo-nacional-de-procedimientos-penales/libro-segundo/titulo-v/capitulo-ii/ . Article 100,	Treated like interception.	**Real-time location tracking and access to stored data:** Article 303, National Code for Criminal Procedure.

	National Guard Law (*Ley de la Guardia Nacional*).		
Panamá	Article 29, Panamanian Constitution. Articles 311, Criminal Procedure Code, https://vlex.com.pa/vid/codigo-procesal-penal-42484053?_ga=2.6352948.721673092.1580504836-202611048.1580504836 . Article 24, Law 121/2013, https://natlex.ilo.org/dyn/natlex2/r/natlex/fe/details?p3_isn=95580 .	Article 310, Criminal Procedure Code. Relevant ruling of the Supreme Court of Justice on July 17th, 2007, https://vlex.com.pa/vid/accion-inconstitucionalidad-suprema-pleno-31663428?_ga=2.7846196.721673092.1580504836-202611048.1580504836 . See also Articles 314 and 317, Criminal Procedure Code. Articles 24, 25, and 47, Law 121/2013.	**Data stored in seized devices not deemed "electronic correspondence":** Article 314 and 317, Criminal Procedure Code. Article 25, Law 121/2013. **Retained traffic data, subscriber data, and location data:** Law 51/2009, https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf .
Paraguay	Article 36, Paraguayan Constitution. Articles 89 and 90, Law 642/1995, http://www.bacn.gov.py/leyes-paraguayas/2452/ley-n-642-telecomunicaciones . Article 200, Criminal Procedure Code, http://www.bacn.gov.py/leyes-paraguayas/203/ley-n-1286-codigo-procesal-penal . Articles 88 and 89, Law 1881/2002, http://www.bacn.gov.py/leyes-paraguayas/4423/ley-n-1881-modifica-la-ley-n-1340-del-22-de-noviembre-de-1988-que-reprime-el-trafico-ilicito-de-estupefacientes-y-drogas-peligrosas-y-otros-delitos-afines-y-establece-medidas-de-prevencion-y-recuperacion-de-farmacodependientes	See also Article 198, Criminal Procedure Code.	Supreme Court of Justice, Ruling n. 674/2010 (*RECURSO EXTRAORDINARIO DE CASACIÓN interpuesto por la Defensora Pública Sandra Rodríguez Samudio en la causa ANASTACIO MIERES BURGOS y otros s/ SECUESTRO y otros*), https://www.csj.gov.py/jurisprudencia/
Peru	Article 2 (10), Peruvian Constitution. Articles 230-231, Legislative Decree 957 (Criminal Procedure Code). Law 27697. Protocol of joint	See also Articles 226-229, Criminal Procedure Code.	Legislative Decree 1182, amended by Law 21284/2021.

	action, implemented by Ministerial Order Nº 0243-2014-JUS (*Protocolos de Actuación Conjunta – Resolución Ministerial n. 0243-2014-JUS*)		
Elements considered as factual basis for law enforcement access to communications data		See highlights of such elements in Argentina, Brazil, Chile, Colombia, Mexico, Panama, Paraguay, and Peru .	

As the table shows, countries generally require some form of judicial oversight to access data like IP addresses and location data, though the specifics vary. Exceptions exist where law enforcement or prosecutorial authorities can access communications-related data without prior judicial authorization, usually with subsequent judicial review (e.g., Colombia, Panama, Peru). While the need for a previous judicial order for accessing the content of communications is almost unanimous among analyzed countries, except for Colombia and the emergency provision in Argentina, disclosure of metadata still receives a lower degree of protection in some countries.

Peru allows real-time location data access without a warrant under specific conditions set in Legislative Decree 1182, subject to later judicial review. In Panamá, Law 51/2009 authorizes prosecutors to request a considerable amount of communications metadata to telephone providers and ISPs with only subsequent judicial review. In Paraguay, a 2010 Supreme Court of Justice ruling hinders the application of stronger safeguards for law enforcement access to communications data. Ruling 674/2010 held that Paraguay's constitutional protection of communications covers only the content of communications, so prosecutors can request call records, telephone subscriber identification information, and location data without a previous judicial order. Law enforcement authorities in Paraguay rely on this ruling to require access to metadata without judicial authorization, even though the country's Telecommunications Law 642/95 says that both the contents and the existence of communications cannot be disclosed except by court order. In Brazil, there's ongoing legal debate on whether the disclosure of stored location data requires a previous judicial order.

Subscriber data tend to have still less stringent protections compared to location data and other metadata. Subscriber information is crucial to identify internet users, by connecting IP addresses, user accounts, and other online identifiers to identification information, such as name and address. Generally deemed less sensitive in the researched countries, subscriber data is the link between someone's identity and their activities online and offline (through GPS coordinates, for example). This can be used to create a nicely detailed police profile of a person's daily habits and relations or reveal an otherwise anonymous journalistic source. The lack of proper safeguards poses a threat to the safety of activists, human rights defenders, dissidents, journalists, and everyday people likely

to face persecution and reprisals for countering and criticizing entrenched powers. Requiring a prior and reasoned judicial order[24] to disclose online identities, following necessary and proportionate principles, is paramount to prevent abuses and aligns with the Inter-American Court on Human Rights' case law.[25] Yet, many Latin American legal frameworks still fail in that regard.

(b) Legal Basis for Government Use of Malware

Regarding law enforcement use of malware, our 2020 research found that none of the eight Latin American countries featured clearly authorized malware as an investigative tool, despite the government's widespread use of such technology. Malware or malicious software seeks to gain access or damage a device without the owner's consent. Malware includes spyware, keyloggers, viruses, worms, or any type of malicious code that infiltrates a computer system. Malware is known to be used or have been purchased by government entities at least in México, El Salvador, Brazil, Paraguay, Panamá, Colombia, Chile, Ecuador, and Honduras with insufficient legal authorization. In certain countries, law accounts for the possibility that some authorities may require judicial authorization for the intervention of private communications, and that might be the legal authority employed by some governments to use malware.

For example, in Paraguay, Article 200 of the Criminal Procedure Code states a judge may authorize the intervention of the communication "irrespective of the technical means used to intervene it." In Chile, Article 24 of the Intelligence Law contains a broad definition of special procedures for obtaining information that such law authorizes. However, constitutional protections and international human rights law must balance legal interpretation grounding any government interference with the right to privacy. Any intervention must comply with a three-step test: be properly prescribed by law; have a legitimate aim; and be necessary and proportionate.

Furthermore, the exploitation of software vulnerabilities by law enforcement and intelligence agencies as standard practice for gathering information is problematic. It incentivizes an "insecurity" market, perpetuating and taking advantage of security flaws unknown by system's manufacturers rather than fostering the responsible disclosure of security flaws so that developers can patch

[24] In the case *Benedik v. Slovenia*, the European Court of Human Rights held that there had been a violation of the right to respect for private and family life when Slovenian police failed to obtain a court order before accessing subscriber information associated with a dynamic IP address. According to the Court, the legal provision used by the Slovenian police to access subscriber data associated with the IP address, without first obtaining a court order, had not met the European Convention on Human Rights standard of being "in accordance with the law." See the ruling at https://hudoc.echr.coe.int/eng#%7B%22itemid%22:[%22001-182455%22]%7D .

[25] Particularly, Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment of October 18, 2023, paras 551, 553, and 554.

them. Governments must recognize that intelligence agency and law enforcement hostility to device security is dangerous for those they aim to protect. We must have strong security at the start and strong accountability after the fact if the goal is to ensure that everyone can enjoy cyber and communications security.

(c) Other Concerning Trends

Direct Access

Direct access to telecommunications companies' networks for intercepting communications or obtaining communications-related data is a problematic government surveillance practice reported in some Latin American countries. Millicom's global transparency report highlights that direct access requirements in Honduras, El Salvador, and Colombia prevent ISPs from even knowing how often or for what periods interception occurs. Millicom reports that in Colombia, the company is subject to strong sanctions, including fines, if authorities find it gained information about interception via direct access taking place in its system. As a result, Millicom does not possess information regarding how often and for what periods of time communications are intercepted in its mobile networks. The ISP states that a direct access requirement also exists in Paraguay, but the procedures there allow the company to view judicial orders required for government authorities to start the interception.

The Telecommunications Industry Dialogue emphasized that direct access arrangements can leave companies without any operational or technical control of their technology and customer data. Such arrangements restrict the ability of service providers to possibly scrutinize, question, and report about government access to data. In this sense, the GNI pointed out that direct access practices are troublesome in at last three ways: they are usually not subject to the same legal procedures that mediate and provide oversight of law enforcement requests; authorities tend to implement direct access through tools that go beyond standardized lawful interception solutions; and direct access practices are often not publicly acknowledged or reported. Another crucial aspect the GNI notes is that "in contrast to law enforcement requests, which tend to be target-based, direct access arrangements usually extract data in bulk."

The Office of the High Commissioner for Human Rights (OHCHR) and the European Court of Human Rights (ECtHR) stated that direct access practices are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards. At least in the countries we detailed in the table, not even the legal basis that authorizes direct access procedures is clear. To the best of our knowledge, nothing in Paraguay's legislation explicitly and publicly compels telecom companies to provide direct access. In

Colombia, Fundación Karisma reports that authorities have relied on provisions of Decree 1704 of 2012 to intercept communications without the intervention of the telecom company. There are at least two issues to raise in this regard. First, the norm is a decree, and not a formal law. Second, the language of the decree is unclear on whether it dismisses, or even forbids, the company to take part in the interception procedure and be made aware that the measure is taking place in its own infrastructure.

Because of this practice's great risk to unfettered surveillance, direct access arrangements should be condemned. They are inherently disproportionate requests, and are not subject to any oversight or other solid safeguards. States should refrain from such practice, while providers should keep shedding light and raising awareness about direct access' inherent risks.

Reverse Searches

Government authorities are increasingly relying on internet and technology companies' databases to conduct mass, suspicionless searches in the context of criminal investigations. From cell tower searches ("tower dumps") to geofence and keyword searches, those requests, often backed by a judicial order, invert the logic of investigating specific suspects based on a reasonable suspicion that justifies the restriction of privacy rights. Rather, *reverse* searches start from a massive pool of communications-related data linked to certain geographical areas or keywords, during a particular period, to establish a pool of possible suspects.

These searches can include the private information of millions of people unconnected to a crime and subject them to further screening with no reasonable justification. Reverse location searches can expose sensitive information, such as the location of a device owner, chilling freedom of expression and endangering privacy and other human rights. For example, Chilean prosecutors asked telecom companies to turn over all mobile phone numbers that had connected to cell towers near five Santiago's subway stations, where fires marked the beginning of the country's 2019 social uprising and protests. By obtaining these phone numbers, it would be possible to identify device owners located in the protest zone and then seek to infer, based only on their location, whether they took part in the protests. Law enforcement authorities in the U.S. have also used geofence warrants for investigating disorders during Black Lives Matter demonstrations.

In addition to issues of legality (such as whether domestic law clearly authorizes this type of search) and suitability (considering this technique may skew the investigation, reverse the burden of proof, and lead to abusive use), reverse searches raise serious proportionality concerns. Harvesting the haystack to possibly find the needle aligns with what human rights bodies understand as mass surveillance and its disproportionate nature. On the contrary, the UN High Commissioner on Human Rights recommended States clarify that authorization of surveillance measures requires reasonable suspicion that a particular individual has committed or is committing a criminal offense or is engaged in acts amounting to a specific threat to national security.

Therefore, reverse searches deserve careful attention from human rights courts and bodies, since they twist procedural safeguards and fail to adhere to standards of necessity and proportionality.

Mandatory Collection of Biometric Data for the Provision of Telecom Services

The use of biometric data, particularly facial recognition, is increasing among mobile service providers, especially for prepaid lines, as a method of verification to activate telecommunications services. Government proposals requiring users to provide biometric data to use mobile telephone services stirred great civil society resistance in México and Paraguay, which was able to suspend its implementation and final legislative approval, respectively.

Conversely, this practice has gained steam in Brazil. InternetLab analyzed ISPs' position on this topic in its 2022 QDTD report. The report found there was little commitment from companies. InternetLab did not find any public document or statement countering the mandatory use of face recognition as a method of verification to activate telecommunications services. Yet, the report positively highlights that Oi does not use the technology to register their users.

Normalizing the processing of biometric data as a condition to activate mobile lines runs afoul of the sensitive nature of this type of personal information. The risks of associating communications and biometric data pose another layer of concern regarding potential arbitrary uses, especially regarding government increasing implementation of face recognition technologies in public security. Face recognition represents an inherent threat to privacy, social justice, free expression, and information security. The disparate impact of this technology on vulnerable groups is among the main reasons that led EFF to advocate for a ban on government use of face recognition systems.

(d) Transparency of Surveillance Measures and User Notification

The questions we address in this section are:

e. Does the state make public information regarding the regulatory framework of surveillance programs; the entities in charge of their implementation and oversight; the procedures for authorizing, choosing targets, and using the data collected; and the use of these techniques, including aggregate information on their scope?

i. Have states enacted any requirements regarding notification of individuals targeted with digital surveillance?

Transparency of Surveillance Law and Practices

Legislation indicated in Table 2 above generally mentions authorities in charge of implementing surveillance measures and the need for previous judicial authorization or subsequent judicial review. The level of detailing varies in pointing out the specific authority within law enforcement agencies. Often, it requires knowing other norms that structure these agencies and distribute related powers and functions. Most of them, especially criminal procedural legislation, contain information on the procedures for authorizing, choosing targets, and using the data collected, but the extent to which they reflect current practices in detail also varies.

Law enforcement agencies' protocols for surveillance that specify and operationalize powers and measures established in law are often deemed secret. For example, while the Peruvian protocols for wiretapping by telecom companies are public, the guidelines on data-sharing by ISPs with police, implementing Legislative Decree 1882, have been declared "reserved information." In Chile, the Public Prosecutor's Office has developed, and ISPs have agreed to, a protocol for communications interception and other data requests that is secret to the general public.

Moreover, under the principle of transparency, States should publish aggregate information about data requests to service providers. Likewise, states should not interfere with companies' efforts to publish records of government requests for user data. The secrecy of specific and ongoing surveillance measures should not prevent the publication of statistical data about government surveillance demands.

Brazil and Mexico have regulations that stand out in this regard. Mexico's 2015 General Transparency Law establishes that the Federal and Local transparency laws require obligated subjects to regularly disclose statistical information about data demands made to telecom providers for interceptions, access to communications records, and access to location data in real time.[26] Brazil's decree 8.771/2016 obliges each federal agency to publish, on its website, yearly statistical reports about their requests for access to internet users' subscriber data. The statistical reports should include the number of demands, the list of ISPs and Internet applications from which data has been requested, the number of requests granted and rejected, and the number of users affected. Yet, there are challenges regarding authorities' compliance with this provision. On a positive note, Brazil's National Council of Justice created a public database with statistics on requests for breach of communications secrecy authorized by courts. While it focuses on

[26] See Article 70, XXX and XLVII.

communications interception procedures, it would be important to also include the disclosure of other types of communications data.

User Notification

The notification of individuals targeted with digital surveillance is a major challenge. The years of QDTD reports have shown how difficult it was to get ISPs commitment to notify users about government data requests.[27] ISPs often argue that user information requests by law enforcement authorities are subject to secrecy duties, and it's hard for them to know when their secrecy obligations end so as to notify targeted users.

Although the obligation to notify falls primarily on the State, ISPs' voluntary commitment to inform users about government data requests, when they are not forbidden by law from doing so, is a key element of creating a culture of transparency and protection of essential privacy safeguards. Many Latin American countries have laws that establish that communication interception procedures are by default secret. But some, like Chile and Perú, have clear obligations to notify users within conditions set by law. Others, like Argentina, do not address the issue of notification after the conclusion of an investigation. Prior notification of digital surveillance measures is normally ruled out either in law or in practice.

While in criminal proceedings the subject of the investigation may learn about the surveillance measure if it led to evidence used in the criminal case, the situation is worse when it comes to intelligence activities. In Argentina, an important Supreme Court case recognized individuals the right to request access to the information that has been gathered on them by intelligence agencies. In the *Ganora* decision, the court stated that intelligence officials cannot reject requests made by individuals for access to information about themselves using a blanket exception. On the contrary, the Supreme Court requested intelligence authorities to justify any exception for accessing information.[28]

Governments must notify individuals who have been subjected to secret surveillance measures, even if such notification is provided after the surveillance has occurred. Notification is crucial in safeguarding individuals' rights, regardless of where the individual resides, enabling them to challenge unlawful surveillance or seek remedies for abuses. Both the ECtHR and the European Court of Justice (ECJ) have consistently underscored the importance of this safeguard.

[27] See more in "User Notification" at https://www.eff.org/wp/who-defends-your-data-latin-america-spain-comparative-view-telecom-companies-commitments-user#Regional .

[28] Supreme Court of Argentina. Ganora s/ hábeas corpus. Decision of September 16, 1999. The Supreme Court ratified this doctrinal line in the R.P., R.D. decision of 2011 (Supreme Court of Argentina. R.P, R.D. c/ Secretaría de Inteligencia. Decision of April 19, 2011).

In its *Weber* judgment, the ECtHR emphasized that individuals cannot effectively pursue legal recourse unless they are made aware of the surveillance measures against them. The Court further noted that the lack of such notification undermines the ability of individuals to challenge the legality of these measures, thereby weakening their right to seek redress.

Similarly, the ECJ ruled that effective judicial oversight of secret surveillance is fundamental to upholding the rule of law. In one landmark judgment, the Court held that without access to personal data or notification of its collection, individuals are deprived of the right to seek rectification or erasure, thereby violating their fundamental right to judicial protection.

Various legal frameworks globally recognize the necessity of notification provisions, as seen in countries such as Austria, Canada, Finland, Germany, South Korea, and Switzerland. These countries provide mechanisms where individuals are notified once the surveillance no longer jeopardizes its purpose. For example, Estonia and Belgium permit notification only when it will not endanger the investigation, and other countries, like Switzerland, allow judicial discretion in determining whether notification is justified.

Relatedly in the Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, the Inter-American Court has drawn on international case law about the notification of individuals targeted by surveillance to highlight the need for ensuring proper mechanisms to provide effective remedy and redress for those affected by arbitrary government surveillance.[29]

(e) Challenges for Robust Oversight

The questions we take into account in this section are:

> d. What ex ante and ex post oversight procedures are in place for use of digital surveillance techniques? Do independent oversight bodies monitor state digital surveillance activities? What if any due process guarantees are provided?
>
> k. How have consumer protection or data privacy authorities within OAS states addressed the misuse of digital surveillance technologies?

[29] Case of Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment of October 18, 2023, para 565.

Table 1 provides a snapshot of judicial oversight in the context of criminal investigations in the featured countries. As pointed out in section 2 (a) of this submission, prior judicial authorization is usually required for accessing communications content. A notable exception to this is Colombia, where the Office of the Attorney General can request the interception of communications without prior judicial authorization but is subject to subsequent judicial review. Yet, the clear need for a previous judicial order is reduced when it comes to the disclosure of other communications data (see section 2 (a)). Proper judicial oversight also involves having clear guidelines set by law and jurisprudence to guide courts' analysis on whether surveillance measures are suitable, necessary, and proportionate. While communications interception legal frameworks tend to have more clear criteria in that regard, such as limiting this type of surveillance to the investigation of serious crimes, this is less the case for the disclosure of other communications-related data.

Due process guarantees are generally embedded in the legal frameworks for the production of evidence in criminal investigations but also depend on the strength of constitutional protections in each country's judicial system. As pointed in section 2 (d), adequate oversight and due process guarantees are even more challenging in the context of intelligence activities. Some countries in Latin America combine judiciary and legislative control of intelligence agencies. However, making this control truly effective, with sufficient powers to oversee activities and punish abuses, is also a key issue. Our 2016 reports in collaboration with allies have taken a closer look at national intelligence systems and related legislation, including challenges for appropriate oversight.[30]

A major hurdle for ensuring proper independent oversight of government surveillance activities relates to limitations in applying data protection legal frameworks to law enforcement, national security, and intelligence activities. Provisions exempting the application of data protection rules are found in countries like Brazil, Colombia, Peru, and Panamá. Yet, in cases where *habeas data* and/or data protection have the status of constitutional safeguards, individuals have an additional instrument to vindicate their rights before law enforcement and intelligence agencies. Finally, the lack of sufficient autonomy, powers, and resources (both human and financial) of data protection authorities is another barrier to relying on them as a vital piece in a broader oversight ecosystem of government surveillance.

[30] See, for example, Perú's 2016 report, section III.2, available at https://necessaryandproportionate.org/country-reports/peru/twenty-sixteen/ and Argentina's 2016 report, available at https://necessaryandproportionate.org/country-reports/argentina/twenty-sixteen/ . See also, INTERNETLAB. O direito das investigações digitais no Brasil: fundamentos e marcos normativos, 2022, section 2.8, available at https://internetlab.org.br/wp-content/uploads/2022/10/INTERNETLAB_O-DIREITO-DAS-INVESTIGACOES_PRINT_10-2022.pdf

(f) From Global to Local: Cross-Border Surveillance and The Risks Introduced by the UN Cybercrime Treaty in Latin American Countries

The UN Cybercrime Convention compounds the challenges presented in two ways. First, it establishes domestic surveillance powers without incorporating the necessary human rights safeguards in line with international human rights law, such as the principle of legality, necessity, and non-discrimination. These omissions fail to remedy the deficiencies identified in the data disclosure legal frameworks above, leaving significant gaps in protection against unlawful or arbitrary surveillance. Second, Chapter 5 of the UN Cybercrime Convention addresses International Cooperation. The chapter lays out the framework for States Parties to assist in investigations and prosecutions related to cybercrime, as well as in the collection and sharing of electronic evidence. This last cooperation extends to serious crimes, not limited to those involving technology, and includes provisions for the preservation, disclosure, and seizure of data, extradition of offenders, and transfer of criminal proceedings. It also authorizes police sharing information across borders, conducting joint investigations.

Specifically, it mandates countries to engage in cross-border data sharing for a broad range of serious crimes, often without sufficient safeguards. It compels countries to collect and share electronic data across borders, effectively requiring them to assist each other in electronic surveillance for a wide range of “serious” crimes. The cross-border evidence gathering applies to any crime that a state chooses to punish with at least four years of imprisonment under its national law, subject to certain restrictions. Proposals to constrain the definition of “serious crimes” in line with human rights law, “as crimes that threaten bodily harm or significant financial interests” were not adopted, meaning that states might apply the label without any consideration of proportionality and decide for themselves what crimes qualify for global surveillance cooperation. While Article 24 imposes some limited conditions and safeguards on surveillance powers, its application is limited. Specifically, Article 24 only applies if a state is using a power covered by Chapter IV (Procedural Measures and Law Enforcement) when responding to a request under Chapter V (International Cooperation). This means that much of the police cross-border evidence sharing contemplated by the Convention is authorized without any meaningful conditions and safeguards at all. As a result, the treaty may allow—and even require—cross-border sharing of evidence obtained through methods that could be considered abusive or highly intrusive.

This is particularly concerning in Latin American countries, where the lack of adoption of legal safeguards against data demands as shown above, the absence of comprehensive data protection laws in the law enforcement content, and the insufficient mechanisms for transparency, notification, effective remedy, and oversight pose significant risks to human rights and vulnerable communities. To address these challenges, a strong and broad coalition of states and civil society organizations should be formed to coordinate a response to this treaty. Countries should be urged to vote 'no' at the UN General Assembly (UNGA) and, if the treaty is passed, to coordinate efforts to prevent its ratification unless stronger safeguards are included.

5. Gaps, best practices, and recommendations.

Regarding legal, policy, or regulatory trends crystallizing in this space (question (a)), please see our responses to sections 1 and 2 of the Consultation Questionnaire.

(a) Transnational Repression

Digital surveillance technologies, particularly spyware, have increasingly become tools for transnational repression. Governments use these technologies to monitor, harass, and suppress dissidents, journalists, human rights defenders, and political opponents across borders. Spyware has been deployed to surveil individuals outside the targeting country, effectively extending state repression beyond national borders. Such surveillance undermines human rights, including privacy, free expression, and freedom of assembly, and could contribute to arbitrary arrests, detentions, and even extrajudicial killings.

The UN Cybercrime Treaty raises concerns that it might enable broader misuse of these surveillance technologies by mandating cross-border data-sharing and surveillance capabilities without sufficiently robust human rights safeguards. As Kate Robertson explains in her *Lawfare* article, Articles 28, 29, and 30 of the UN treaty call for the real-time interception of digital data, and Article 47(2) endorses direct cooperation between law enforcement agencies across borders—without adequate protections to prevent the use of mercenary spyware or safeguard against the misuse of collected data for repressive purposes.

As Robertson explains, the UN Cybercrime Convention mandates that "signatories adopt surveillance and interception capabilities that can be weaponized by countries seeking legal cover to justify their use of commercial spyware." For instance, Robertson highlights that "Article 28 obliges signatories to obtain surveillance capabilities over stored electronic data in their territory, and Articles 29 and 30 compel states to implement real-time interception of traffic and content data". She added:

> Notably, the provisions do not prohibit states from turning to cyber mercenaries wielding commercial spyware to obtain the requisite capabilities. A state could, under the aforementioned articles, argue that the treaty allows states to turn to commercial spyware vendors for the requisite surveillance capabilities.

(b) Recommendations

Our recommendations build on the Necessary & Proportionate principles drafted upon international human rights law. As such, and according to Inter-American Human Rights standards, any limitation to privacy must be prescribed by law, and the law must be sufficiently accessible, clear, and precise so that individuals have advance notice of and can foresee its application. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available.

Any privacy permissible limitation must not undermine the essence of the right itself and must align with other human rights, including the principle of non-discrimination. This ensures that surveillance measures do not disproportionately affect certain groups based on race, gender, ethnicity, or political beliefs, a core concern especially in contexts where marginalized communities are more vulnerable to invasive state surveillance. If these criteria are unmet, the limitation would be unlawful, and any resulting interference with privacy would be arbitrary. The States' duty to respect and ensure the right to privacy entails the proper adoption of procedural safeguards and effective oversight of government surveillance powers.

Based on that, we highlight the following recommendations for States:

- Establish comprehensive and effective data protection legal frameworks. Ensure solid and independent oversight powers and structure to data protection authorities. Data protection legal frameworks and the mandate of oversight authorities should apply both to private parties and state parties, including law enforcement and intelligence agencies.
- Publish transparency reports of government demands to access customers' information. The UN Special Rapporteur for Freedom of Expression has called upon States to disclose general information about the number of requests for interception and surveillance that have been approved and rejected. Such disclosure should include a breakdown of demands by service provider, investigation authority, type and purpose of the investigation, number of individuals or accounts affected, and period covered. States should not interfere with service providers in their efforts to publish records of government data requests and the procedures they apply when assessing and complying with such requests (see Principle 9).
- The baseline for any government policy involving data processing affecting persons and/or groups should include robust nondiscrimination and data protection rules, with safeguards like data minimization, purpose limitation, and consent. It should also involve concrete and effective measures to ensure security, transparency and accountability, and community control, and that data-intense policies are legitimate, necessary, and efficient. This includes meaningful civic participation on whether and how these policies should be conceived, implemented, or maintained.
- Review legislation to ensure they establish strong privacy safeguards for government access to data vis-à-vis the current technological landscape and the deeply powerful surveillance capabilities it enables. Domestic legislation should specifically

restrict investigative powers in scope and duration to specific criminal investigation and prosecution. It should require a prior judicial authorization by a judicial authority that is impartial and independent before law enforcement gain access to user data. Subsequent judicial review should only apply in cases of emergency when there is imminent risk of danger to human life.

- Encourage all states to implement independent, prior judicial authorization for any surveillance measures, especially those involving communications data (metadata and subscriber data). Surveillance should be based on reasonable suspicion and follow principles of necessity and proportionality, in line with international human rights standards. States must treat metadata as sensitive and ensure it is subject to the same legal requirements as accessing the content of communications, such as judicial authorization and proportionality tests. States should not rely on artificial categorizations of data (e.g. "subscriber data" or "metadata") to waive prior judicial authorization or to justify any disproportionate interference with privacy. Interferences with users' privacy should also be based on solid evidentiary showing. States should ensure effective redress mechanisms and rigorous judicial oversight by an independent regulatory body.
- Urge states to publish regular transparency reports. These reports should detail the scope, nature, and frequency of data access requests, as recommended by the UN Special Rapporteur for Freedom of Expression in previous reports. States should also refrain from placing undue restrictions on companies' efforts to publish transparency data. This will promote public oversight and accountability while ensuring that surveillance practices adhere to international human rights standards.
- Establish and/or effectively implement a State's legal obligation to notify all individuals affected by government surveillance measures. Such notice should occur with enough time and information to enable them to challenge the decision or seek other remedies. Delay in notification is only justified when it would jeopardize the investigation or prosecution, or imply an imminent risk of danger to human life. The competent judicial authority should authorize such a delay in each case and ensure the user affected is notified as soon as the risk is lifted. States must adopt legal measures to ensure that gag requests—confidentiality and secrecy requests—are not inappropriately invoked when law enforcement make data access demands. In this sense, any measures preventing a service provider from voluntarily notifying users should be exceptional, limited in duration, and subject to strict criteria with clear and compelling reasons for imposing such restrictions. Otherwise, deprived of the knowledge about an intrusive measure, the individuals targeted rest with very little or no resources to fight or seek redress against unlawful or arbitrary surveillance.
- Abandon the condemnable practice of adopting secret rules, protocols, and interpretations of law in the context of government access to data. Governments conducting surveillance must ensure that they do so in accordance with a domestic legal framework that meets the standards required by international human rights law. As such, any legislation governing surveillance must be clear, precise, and publicly accessible.[31]

[31] See UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021). See also Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/27/37 (30 June 2014), paragraph 29; and

- Cease disproportionate surveillance mandates. Governments should not require service providers to grant direct access to their networks or servers. Indiscriminate, suspicionless searches targeting communications data also fail to meet necessary and proportionate standards. National courts and lawmakers should not support or connive with such practices. On the contrary, national case law and legislation should uphold international human rights standards and constitutional norms by ensuring sufficient safeguards to curtail arbitrary and disproportionate government surveillance.
- Indiscriminate surveillance is inherently disproportionate. Such practices are incompatible with international human rights standards, particularly the right to privacy and the protection of personal data, including the Inter-American Human Rights System. It should be equally repelled by national law. Data collection should be narrowly tailored and restricted to specific, targeted investigations where there is credible evidence of criminal activity
- Explicitly guarantee that domestic legal frameworks recognize biometric data as categorically personal sensitive in all instances, that should be treated with the highest levels of protection. Accordingly, States should abandon inherently disproportionate processing of biometric data, such as government use of face recognition. In addition, States should refrain from setting facial recognition and other biometric data collection mandates for users' to activate and benefit from telecommunications services.
- Urge states to adopt and enforce legal frameworks that protect the use of strong encryption. Surveillance measures that undermine encryption can expose users, including vulnerable communities and human rights defenders, to surveillance and cyber-attacks. States should refrain from mandating backdoors in encryption systems, in line with the UN Special Rapporteur's recommendations on the use of encryption to protect freedom of expression.
- Digital surveillance laws must include enhanced safeguards for groups that perform a public watching role, such as NGOs, journalists, and activists, akin to the protection afforded to lawyers-clients, and the press and its source. Access to their data should be subject to stringent prior judicial authorization, with limits on data retention, access and destruction to prevent misuse.
- Ensure that individuals subjected to secret surveillance measures have the opportunity to claim victim status, even when they are unaware of the specific measures taken against them. Legal frameworks should allow for the presumption of victimhood when applicants can reasonably demonstrate that they belong to a group likely targeted by the surveillance legislation or are affected by general surveillance practices. Additionally, effective domestic remedies should be available, including the right to subsequent notification of surveillance measures, which is essential for enabling individuals to seek redress.

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc A/HRC/41/35 (28 May 2019), paragraph 50.