Who Defends Your Data in Latin America & Spain?

A COMPARATIVE VIEW OF TELECOM COMPANIES' COMMITMENTS TO USER PRIVACY

ELECTRONIC FRONTIER FOUNDATION

Author: Veridiana Alimonti
Editor: Karen Gullo

EFF's Policy Director for Global Privacy, Katitza Rodriguez, reviewed this report. EFF's Design Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade, formatted this report. We also thank all partner organizations in the *¿Quién defiende tus datos?/¿Dónde están mis datos?* project for the sustained series of reports and years of collaboration. These organizations are: Fundación Karisma, Hiperderecho, R3D, InternetLab, Derechos Digitales, TEDIC, ADC, Eticas, and IPANDETEC.

A publication of the Electronic Frontier Foundation, 2023.

View this report online:
https://www.eff.org/wp/who-defends-your-data-latin-america-spain-comparative-view-telecom-companies-commitments-user

Who Defends Your Data in Latin America & Spain?

A COMPARATIVE VIEW OF TELECOM COMPANIES' COMMITMENTS TO USER PRIVACY

VERIDIANA ALIMONTI
Associate Director for Latin American Policy

MAY 2023

Introduction

This report presents an overview and comparative analysis of the *¿Quién defiende tus datos?/¿Dónde están mis datos?*[1] series of reports for Argentina, Brazil, Chile, Colombia, México, Nicaragua, Panamá, Paraguay, Perú, and Spain. Since 2015, local digital rights organizations have evaluated telecommunications companies' commitments to transparency and user privacy in a regional initiative inspired by EFF's *Who Has Your Back (Government Data Requests)* project.

Internet and telephone service providers have access to users' sensitive, private information detailing much of their daily activities—from what videos they share on social networks, what websites they visit, and when they log in to online services, to their whereabouts offline through location data. This can reveal intimate details of users' lives, movements, actions, relations, habits, and interests. Internet and telephone services companies are often asked by government and law enforcement agencies to turn over user information. The choices companies make in responding to these requests affect the privacy of every one of their users, and how they generally collect, use, and share user information is vital to ensure users' rights. As such, they should have the strongest possible protective, transparent policies and practices to shield user data from unwarranted and unjustified government and corporate surveillance.

Under international human rights standards, companies have a responsibility to ensure that their practices respect fundamental rights, including the right to privacy. That responsibility exists independent of whether a State meets its own human rights obligations. As the Office of United Nations High Commissioner for Human Rights (OHCHR) pointed out in its first report about the right to privacy in the digital age,

> *[w]here enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honor the principles of human rights to the greatest extent possible, and to be able to demonstrate their ongoing efforts to do so. This can mean interpreting government demands as narrowly as possible, seeking clarification from a government with regard to the scope and legal foundation for the demand, requiring a court order before meeting government requests for data, and communicating transparently with users about risks and compliance with government demands.*

With these standards in mind, *Quién defiende tus datos* (QDTD) reports have been conducted in 10 countries to push telecom providers to embrace privacy and data protection best practices.

The key network of organizations leading local reports over the years include:

Fundación Karisma (Colombia), first edition published in 2015.

Hiperderecho (Perú), first edition published in 2015.

R3D (México), first edition published in 2015.

InternetLab (Brazil), first edition published in 2016.

[1] ***Who Defends Your Data?/ Where Is My Data?***

Derechos Digitales (Chile), first edition published in 2017.

TEDIC (Paraguay), first edition published in 2017.

ADC (Argentina), first edition published in 2018.

Eticas (Spain), first edition published in 2018.

IPANDETEC (Panamá and Nicaragua), first edition published in 2019 and 2020, respectively.

With four sections, this report outlines the main findings of our partners' studies through a broad, regional lens. The first section explains the projects' main criteria, provides general highlights on results over the years, and compares the performance of regional and/or global telecom companies in countries covered by the project. The "'second section looks at what QDTD reports reveal about problematic trends and challenges in the region vis-à-vis the much-needed application of human rights standards to government access to data. The third section briefly discusses companies' advances and weaknesses in data protection frameworks as reflected in the reports. Finally, the fourth section outlines conclusions and recommendations.

1. An Overview of QDTD Reports

1.1. Methodology and Main Common Criteria

The QDTD reports in Latin America and Spain mainly focus on local and regional telecommunications and broadband service providers. The reports look at national markets and aim to encourage companies to adopt strong user privacy commitments to gain a competitive advantage, as customers are increasingly concerned about data protection. Some of the featured companies are major regional or global players providing services through local branches or affiliates, like Telefónica (Movistar/Vivo), América Móvil (Claro), Millicom (Tigo), and AT&T (DirecTV). Others are local, independent internet providers.

A lot goes into releasing a QDTD report. First, experts from local partner organizations identify key local Internet Service Providers (ISPs), and then sift through their publicly available terms of service, privacy policies, transparency reports, and law enforcement guidelines. In addition, the experts engage with the companies directly to garner more details and feedback about their policies. This engagement also allows experts to keep tabs on whether companies are fighting for their users in court, Congress, and in public policy debates.

Evaluation criteria are adapted to fit local laws and realities, and companies are granted scores, usually stars, for their best practices and commitments. Stars are generally given based upon publicly available information that any Internet user can access and verify. Partial compliance with evaluated practices and policies lead to partial stars, according to each report's methodology.

The evaluation criteria often change from one country to the next. Nonetheless, the criteria focuses on three main issues: public commitment to comply with privacy safeguards; the adoption of pro-user practices and policies; and transparency. Overall, the parameters evaluate:

Data Protection Policies: Does the company have a copy of its internet service contract and/or its data protection policy published on its website? Over the years, reports made the evaluation stricter, detailing specific information ISPs should provide in their policies.

Transparency: Does the company regularly publish a transparency report? Assessed parameters vary, but many reports check whether the company discloses the type of user data requested (content, metadata, subscriber data, location data, device IDs, among others), along with the aggregate number of government requests the ISP received, fulfilled, and rejected.

Law Enforcement Guidelines: Does the company publish the procedure, requirements, and legal obligations the government should comply with when requesting personal information about its users?

Judicial Authorization: Does the company commit to apply local law according to the most protective interpretation of safeguards, such as requiring a judicial order before handing user data to authorities.

User Notification: Does the company commit to notifying users about government requests for information, and/or take concrete steps to make it possible to serve such a notification for its users?

Commitment to Privacy in Courts/Legislative or Policy Venues: Has the company defended privacy and actively protected users' data, either in court or as part of a legislative discussion in Congress?

Digital Security: Does the company adopt proper digital security measures? Some QDTD reports check the use of encryption (HTTPS) on ISPs' communication channels and payment functionalities. Over the years, some reports have also checked whether ISPs adopt other security measures, provide digital security content to users, and publish the company's policies on cybersecurity and/or data breaches.

1.2. Highlights of Achievements and Gaps

The assessments have evolved since the project's first editions. While certain parameters have become consolidated industry best practices (e.g. periodic publication of transparency reports) or specific legal obligations (e.g. making data protection policies available to users), some companies' performance still lags, and improvement in some categories remains a persistent challenge. This section maps out what we can capture through QDTD reports from project partners and other initiatives[2] aimed at pushing companies to uphold human rights and user privacy and advocating for critical advances in legislation and case law in recent years.

Data protection policies

Data protection laws setting transparency obligations over the processing of user data certainly play a relevant role in getting companies to disclose information on how they collect, use, and share users' personal and communications data. Yet, QDTD reports have shown a mixed relationship between legal obligations and best practices for this evaluation category.

The existence of data protection frameworks in force did not necessarily correspond to accessible, easy to understand, and comprehensive data protection policies. All three first editions published in 2015 came from countries with data protection laws in place (Colombia, México, and Perú). And in all three reports, companies scored poorly, either for having policies that are difficult to find or understand, failing to include relevant information about personal data processing, or failing to publish any policy at all.

Over time, QDTD reports have shown significant progress not only in *what* information ISPs provide but also in *how* they provide that information. For example, the great majority of companies evaluated in Brazil now have *Privacy Centers* or *Privacy Portals* that gather relevant details on user privacy and data processing, and display that information in a more user-friendly way. Telefónica and América Móvil make such portals available on their local websites in different countries where they operate, although América Móvil still fails to do so in all countries covered by QDTD reports. Section 1.4 details this regional disparity. ADC's Argentina's latest report notes, however, that companies still can do better when organizing the information in such

[2] We can mention, for example, the Global Network Initiative (https://globalnetworkinitiative.org/) and Ranking Digital Rights' reports (https://rankingdigitalrights.org/).

portals to make sure users don't have to browse through several sections to access what is most relevant to them.

In Spain, Eticas' report, following enforcement of the EU General Data Protection Regulation (GDPR) and the related Spanish Organic Law 3/2018, indicated meaningful positive changes in the content of companies' policies available online. Some companies, for example, provide contact details for data protection officials and disclose their practices regarding data-based, nonhuman decision making and/or profiling. In contrast, despite the presence of data protection laws in force in Panamá and Nicarágua, ISPs in these countries fail to publish comprehensive data privacy policies for their telecom and internet services. In many cases, policies, when available, only relate to data collection through ISP's own communications channels, such as websites and apps. Not even Millicom's and América Móvil's global data protection policies were found on Panamá's and Nicaragua's local branches' websites. On the other hand, TEDIC's reports on Paraguay have shown improvements in this category over the years, despite the absence of comprehensive data protection legislation.

Finally, Hiperderecho's latest study in Perú checked whether telecom companies published policies or provided customer service channels in native languages, such as Quechua and Aymara. The imbalance was evident in the results. While all four featured companies received full stars for their general data protection policies in Spanish, only Telefónica-Movistar earned a full score in the native language's category.

⇨ See in more detail the information provided in evaluated privacy/data protection policies in **Section 3**.

Transparency Reports and Law Enforcement Guidelines

Companies' *transparency reports* often disclose statistical information and different levels of qualitative information about government requests for user data during a specific period in countries and/or regions where they operate. *Law enforcement guidelines* (LE guidelines) establish the steps authorities should follow to request user data and companies should take locally when responding to authorities. Applicable local law about government demands, types of user data requested, competent authorities to request data, and insights on how companies interpret local legislation and safeguards may be found in transparency reports and LE guidelines, although their main scope differs.

QDTD research indicates that publishing transparency reports is both a settled practice and a persistent gap, depending on which ISP or country we consider (see more details in Section 1.4).

Regarding major telecom companies in the region, we can highlight that:

- **AT&T (including DirecTV),** a US-based company that operates globally through subsidiaries in many countries, has issued transparency reports since at least 2015. The last published report (about requests in 2021/2022) is quite detailed about legal demands related to the US, but provides very little information about requests received by its subsidiaries in other countries. The section about México is a positive exception—the ISP gives some insight into the Mexican legal framework for data requirements, including wiretaps and requests for historic information and location information in real-time. It breaks down statistical data of law enforcement requests into demands for historic

information (subscriber data, call detail records, cell site location information, and identification data of mobile devices), real-time location information, and wiretaps. It also reveals the number of demands rejected/challenged or partially responded to. Regrettably, for all other countries in Latin America and beyond, AT&T only provides the number of data requests received.

- **Telefónica (Movistar/Vivo)** has issued global transparency reports since at least 2016. The last published report (about requests in 2021) breaks down statistical information on government authorities' requests *per country* and per the following indicators: lawful interceptions (including requests for new interceptions, extensions, or to disconnect an existing interception), access to metadata, content blocking and restriction, geographical or temporary suspension of the service, requests rejected or partially dealt with, and number of accesses affected by each request. Telefónica's report also specifies the competent authorities and applicable laws for each type of request in each country.

- **Millicom (Tigo)** has issued global transparency reports since at least 2016. The last published report (about requests in 2022) discloses types and numbers of law enforcement requests received *per region*, not per country, in the following categories: interception, customer metadata, and customer financial data (related to the mobile financial services the ISP provides). The company does not reveal the number of requests it has rejected or complied with. Millicom groups data from countries where the ISP operates into two blocks: *South America* (Bolivia, Colombia, Paraguay) and *Central America* (Costa Rica, El Salvador, Guatemala, Nicaragua, Honduras, Panamá).

  The ISP points out that several countries in which it operates prohibit disclosure of country-specific numbers and that, in their risk/benefit assessment, "even beginning discussions with authorities regarding the disclosure of numbers might [...] lead to negative outcomes for their operations and their ability to promote more rights-respecting practices." However, the legal grounds of such prohibitions are not clear. For example, prior research on legal frameworks in Paraguay, Colombia, and Panamá did not reveal legal prohibitions against publishing aggregate data about government requests. Millicom's global report also does not specify what legislation prohibits publishing country-specific data. In turn, the Global Network Initiative's research about country legal frameworks, cited in Millicom's report and drafted with the ISP's collaboration, mentions legislation in Millicom's covered countries that *does not* specifically address the publication of aggregate data. When explicitly provided by law, prohibitions are in general broadly tailored to address the secrecy of communications and the confidentiality of interception procedures. State authorities and companies should not, as it seems to be Millicom's case, interpret those provisions as preventing the disclosure of statistical information of law enforcement requests for user data. Under applicable human rights standards, preventing companies from publishing such data runs afoul of the critical tenets of transparency and public oversight of government surveillance. Yet, while Millicom falls short of disclosing country-specific statistical data, the ISP's report positively stands out for the qualitative information it provides about local legal frameworks and governments' practices when requesting user data (for instance, Millicom provides a more detailed description about direct access mandates in certain countries—see more below). Millicom's global report also lists the competent authorities that can issue requests for interception and metadata in each country. At the local level, Millicom's

Colombian subsidiary actually publishes a specific transparency report—the only country we found to do so among QDTD studies (see Section 1.4). Interestingly, in such a report, Tigo Colombia discloses government data demands by requesting authority and type of data. For instance, in 2021, the Colombian army made four requests for subscriber data, while intelligence agencies requested subscriber data 10 times and call records six times. The great majority of requests came from prosecutors and the police, followed by courts.

- **América Móvil (Claro)** has taken longer to issue global transparency reports. The first we could find discloses numbers of law enforcement requests in 2020—even though Claro Chile has been publishing a local version since 2018, following QDTD's first edition in the country. There is no easy way to directly access global transparency reports on América Móvil's website. The link is hidden in the ISP's sustainability reports.[3] The company provides statistical information on government data demands *per region*, and not per country, and does not break them down into specific categories of requested data (e.g. interception or customer metadata). It reveals only the total number of requests for user information received from authorities and the proportion of those the ISP complied with. It groups this information into the following regions: *North America and the Caribbean* (United States and Puerto Rico, Mexico, and Dominican Republic), *Central America* (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, and Panamá), *Southern Cone* (Argentina, Brazil, Paraguay, and Uruguay), and *Andean Region* (Colombia, Chile, Ecuador, and Peru). The report does not explain why the ISP does not disclose aggregate data per country, but it does describe the applicable legal framework and competent authorities, as well as provide insights on the company's internal steps for responding to requests. On the latter, the degree of information provided for each country may vary significantly. The report's description of the applicable legal framework is fairly standardized and useful, covering the disclosure of data records to competent authorities, geolocation of mobile devices in real time, interception of private communications, discontinuance of telecommunications services upon court order, and blocking of communication lines used for the commission of criminal offenses. However, the information on competent authorities still lacks clarity and standardization. For Argentina, for example, the report points out only the competent authorities that can request interception of communications. For Paraguay, it generally refers to judges and prosecuting attorneys' offices, with no distinction about requests that only judges can authorize (e.g. interception), unlike the case for Uruguay.

We consolidate this information in the tables below:

[3] América Móvil. Sustainability Report, 2020, at page 95.
https://s22.q4cdn.com/604986553/files/doc_downloads/2021/05/2020-Sustainability-Report.pdf
América Móvil. Sustainability Report, 2021, at page 51.
https://s22.q4cdn.com/604986553/files/doc_downloads/2022/07/AM-2021-SUSTAINABILITY-REPORT-(AI).pdf

ISP	First global report found (year of release)	Statistical data per country or region	Provides number of rejected requests	Provides info on competent authorities	Provides info on legal framework
AT&T	2015	Country	Yes, for México and the U.S.	No	Yes, for México and the U.S.
Telefónica	2016	Country	Yes	Yes	Yes
Millicom	2016	Region	No	Yes	It directs to GNI's Country Legal Frameworks Resource
América Mòvil	2021	Region	Yes	Yes, but it lacks standardization	Yes

ISP	Types of data/requests breakdown
AT&T	México: historic information (subscriber information/call records and cell site information), real-time location information, and wiretaps. Other LatAm countries: subscriber information and IP/URL blocking.
Telefónica	Lawful interceptions (including requests for a new interception, for extensions, or to disconnect an existing interception), access to metadata, content blocking and restriction, geographical or temporary suspension of the service, and number of accesses affected by requests.
Millicom	Interception, customer metadata and customer financial data (related to the mobile financial services the ISP provides).
América Mòvil	No breakdown per type of data/request.

Transparency reports could provide more detail on why companies have rejected government requests and about the proportion of targeted *vs* non-targeted, or massive, requests they received (e.g. requests for mass cell tower data). We explain the latter in more detail below. For now, it is worth highlighting that of the four global reports described above, only Millicom and AT&T directly mention massive or collective requests.

In its report, Millicom says that a request seeking information about several individuals or devices counts as one request in the data table, which means "requests are not equal in magnitude." AT&T explains that while Mexican authorities can request all telephone numbers registered on a particular cell tower for a certain period, the ISP does not keep track of how many telephone numbers it provides to law enforcement in those cases. Both raise a red flag about underreporting of lines, devices, or persons affected by surveillance measures. Telefónica's report includes an additional metric to capture this information by disclosing both the *number of requests* and the *number of accesses affected*.[4] If non-targeted, massive requests are considered, the figures of the former would often be smaller than the latter (for instance, a request for an ISP to disclose all mobile phones connected to a cell tower during a specific day and time is one request that affects hundreds or even thousands of accesses). However, this relation varies throughout Telefonica's report, with countries where the opposite happens or where these two indicators present the same figure. Telefónica could provide further explanation on the relation of both indicators in future reports.

As for reasons that authorities' user data requests are rejected, Telefónica provides a general description in the introductory section of its report.[5] Chilean ISPs started to detail such information in recent years and, since October 2021, Claro Chile disaggregates the number of rejected requests by reason for having rejected them. A significant number of rejected requests don't come from institutional email addresses, or don't present a judicial order, among other problems.

Similarly to transparency reports, there is an increasing trend to consolidate the publication of law enforcement (LE) guidelines as a best practice. Yet, we still see a highly varying degree of information provided. Often, ISPs disclose global summarized guidelines without providing details considering the local law of countries where they operate. This is the case of Millicom and Telefónica, whose transparency reports bring more country-specific information than the LE guidelines that are publicly available. Both companies disclose local LE guidelines, but only for some QDTD countries (see section 1.4).

We could not find LE guidelines for América Móvil, although its transparency report contains some related information, and Claro Chile and Perú publish local guidelines. Vodafone's legal annex stands out for providing thorough information on the applicable law for LE requests in countries where the ISP operates, which includes Spain.

QDTD reports identified and scored local LE guidelines in Argentina (IPLAN and Telefónica-Movistar), Brazil (Algar, TIM, Oi, and Telefónica-Vivo), Chile (all featured

[4] Telefónica's report does not define what the provider means by "accesses" affected but we generally understand the term refers to phone lines or numbers, and mobile or fixed Internet connections provided by the company to its users.
[5] Telefónica explains that rejected requests for user information were denied for the following reasons: they do not comply with local legislation for that type of requirement; they do not contain all the necessary elements (necessary signatures, competent authority, technical description of the requirement, etc.), or it is technically impossible to execute the request.

ISPs), Colombia (Telefónica-Movistar, Millicom-Tigo, ETB and DirecTV), Perú (América Móvil-Claro and Telefónica-Movistar), and Spain (Vodafone).

Transparency reports and LE guidelines are crucial tools for government accountability and public oversight in communications surveillance. They shed light on critical aspects of how government authorities gain access and use customer information, as well as on checks and safeguards companies consider when responding to requests.

Over the years, QDTD reports have encouraged ISPs to level up their commitments and push companies to disclose useful details for identifying and addressing concerning trends. Two such trends are governments' direct access to telecom companies' networks and the use of nontargeted, massive, user data requests and/or data-sharing agreements for criminal investigation, inspection, or policy purposes.

Millicom's transparency report mentions that the ISP must grant government authorities direct access to its networks in Honduras, El Salvador, Colombia, and Paraguay. Considering this and other reports, Karisma included a parameter in Colombia's 2021 edition to assess whether companies disclose information about their direct access practices, such as the authorizing legal basis for direct access, and the ISP's role. According to Karisma's report, Telefónica-Movistar clearly addressed the topic, and both América Móvil-Claro and Millicom-Tigo disclosed information on the legal framework that allegedly underpins direct access in Colombia. Six other companies evaluated in Colombia's 2021 report were silent about this practice. The challenges to properly report about direct access remained in Colombia's latest edition. This time, only Movistar and Tigo received credits in this category.

In turn, the COVID-19 pandemic brought greater attention to massive government requests for user data and/or data-sharing agreements involving telecom companies. It has also reinforced discussions on the sensitivity of location data. See Section 1.3 of this comparative report for more insight on how the pandemic affected QDTD criteria. Yet, InternetLab's reports for Brazil have assessed information ISPs provide on disclosure of geolocation data to authorities since the 2019 edition. More recently, Brazil's 2021 report found that only half of the evaluated companies mention the collection or processing of location data. Of those, just TIM and América Móvil-Claro provide further detail about the circumstances in which they share user location data to authorities and why taking into account the Brazilian legislation applied to this type of data.

As for data-sharing with government entities, Colombia's 2021 report highlighted that a lack of transparency and user notification makes it more difficult to track the misuse of personal data. In addition, state-owned companies (either fully public or with state participation) should be clearer on whether and how they share user personal information for policy or other purposes. Karisma underlines the case of telecom operator ETB, which is one of the owners of Bogotá Data Analytics Agency (*Agencia de Analítica de Datos de Bogotá* – AGATA). AGATA's corporate purpose is to contribute to Bogotá's smart city-related initiatives, and offer services to the private sector. According to its website, the entities that formed AGATA provide data the agency uses to offer digital solutions. ETB does not detail information about this collaboration.

Finally, ISPs still reveal very little about their data-sharing practices and agreements with their business partners, which some QDTD reports have started to track. To take a more holistic look at business practices related to data requests from public authorities, publishing ISPs' data protection impact assessments (DPIA) would definitely improve transparency and public oversight of government and corporate surveillance. Since

Brazil's 2020 report, InternetLab has checked whether companies publish DPIAs, but so far no evaluated company has done so.

- ⇨ See more about transparency challenges and proportionality concerns regarding law enforcement access to data in **Sections 2.1 and 2.3**.
- ⇨ See more on what companies say about their data-sharing with commercial partners in **Section 3.1**.

Judicial Authorization

This evaluation category checks whether the ISP publicly commits to seek a judicial order before handing user data to authorities. Achieving such a commitment depends on what is required or allowed by the domestic legal framework in each QDTD country. The methodology of each report is adapted to reflect ISPs' room to maneuver within the legal framework of each country in adopting protective interpretations when responding to law enforcement requests. While the need for a prior judicial order is almost unanimous among QDTD countries for communications interception, except for Colombia, government access to metadata often enjoys a lower level of protection in the region. When the law gives the same protection to metadata, as in Brazil, or does not make a distinction to undermine metadata safeguards, as in Chile or Argentina, QDTD reports ask for ISPs' commitments to require a judicial order before handing both communications content and metadata. When domestic legislation clearly authorizes law enforcement authorities to access metadata without previous judicial authorization, as in Panamá, QDTD reports reformulate the ask and instead seek information about companies' commitment to refuse unlawful government requests.

In general, QDTD reports found more robust commitments to require a prior judicial order for metadata government requests in Brazil, Chile, Perú (especially Telefónica-Movistar), and Spain (especially Vodafone).

- ⇨ See more on the importance of achieving greater safeguards for government access to metadata in Latin America in **Section 2.2**.

User Notification

Perhaps the most challenging evaluation parameter in QDTD reports is asking ISPs whether they notify users when the government seeks their data, as many companies operating in Latin America resist this practice. They 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, even though this project category asks for ISPs' commitment to notify users at the first opportunity allowed by law. However, in light of ISPs' hesitancy, many QDTD reports give credits when companies demonstrate concrete efforts towards transparency. They can earn credit for engaging with authorities or through other venues to implement a notification procedure for criminal cases, committing to notify users about data requests in other types of cases (e.g. civil, labor, and family cases), or for simply disclosing clear policies regarding user notification.

Over time, QDTD reports played a relevant role in getting ISPs to embrace user notification policies. Project partners identified declarations reserving the possibility to notify users about data requests in Argentina (AT&T-DirecTV, Telefónica-Movistar), Chile (WOM, VTR, América Móvil-Claro, GTD), Colombia (AT&T-DirecTV), and Panamá

(Más Móvil). In Chile and Perú, América Móvil-Claro has committed to notify users in civil, labor, and family cases. WOM has followed suit in Chile.

⇨ See more on the key role user notification of government requests play in human rights safeguards in **Section 2.4**.

Commitment to User Privacy in Courts, Congress, and/or Policy Discussions

This category seeks to measure companies' commitments beyond what they state in their policies, looking at whether ISPs have taken a stance in favor of user privacy before courts, Congress, administrative bodies, or in the context of other policy discussions. However, this is a challenging category to measure and largely depends on companies' engagement with QDTD partners to provide links and documents showing their practices. Telecom companies usually do not report systematically about legal cases they initiated challenging arbitrary data demands or their positions in specific legislative or policy debates regarding privacy. AT&T does publish information about its positions and activities regarding Internet protection and security, but its website content, with few exceptions, addresses only global discussions or US-related events. Telefónica's corporate website also features posts elaborating on policy issues. Yet, there is not much there specifically about Latin American countries.

To evaluate this category, QDTD research generally involves checking media, ISPs' social networks, and their participation in public events. Companies' litigation is also easier to map and identify in countries where searching for case law in various domestic courts is a streamlined task, which varies significantly among QDTD countries. Across QDTD reports, Claro Chile stands out in this project category for creating a specific section on its website to detail interactions with public authorities. In Brazil, Oi includes in the company's sustainability report information about judicial challenges it started against government data requests. Millicom's global transparency report also gives some insight into its engagement with local authorities to strengthen privacy and due process safeguards. When possible, the company could provide more concrete resources related to such efforts.

Companies are in a critical position to assess and curb abusive government requests, especially when there is no previous notification to users and targeted people can only seek remedy after the intrusive surveillance measure has happened. QDTD reports underlined relevant instances where ISPs stood up for user privacy. Here are some examples:

- In Brazil, InternetLab reports highlighted the constitutional challenge filed by the national association of mobile companies (ACEL) against a provision in the country's Criminal Organizations Law allowing disclosure of telephone metadata without a previous judicial order. More recently, the telecom provider Oi challenged a judicial order granting police the power to access all telephone-related stored data for six months, including subscriber information, call and SMS records, and location data. In the latest report, Claro, Oi, TIM, Vivo, and Brisanet directly challenged government data requests because they lacked a judicial order, showed an insufficient legal basis, or went beyond companies' legal obligations to store data.
- In Perú, Hiperderecho reported about Claro's refusal to comply with a request by the country's tax authority SUNAT to disclose the complete database of prepaid and postpaid customers for audit purposes.

- Regarding legislative debates, Derechos Digitales pointed out a communication Claro Chile sent to legislators regarding the reform of Chile's Data Protection Law. The ISP expressed concerns about requests for user information it receives from public bodies, suggesting that personal data processing standards for companies should also apply to state bodies, including preventive controls and compliance officers.

Finally, QDTD reports often give credits to companies in this category if they join multistakeholder initiatives for the protection of users and the promotion of human rights. We should note that major telecommunications companies in the region, such as Telefónica and Millicom, have recently left the Global Network Initiative (GNI), a free expression standard setting project whose members include companies, investors, and nonprofit organizations from different regions. Although Telefónica and Millicom remain part of the Telecommunications Industry Dialogue, a group of telecom operators and vendors promoting free expression and privacy, this initiative is comprised of companies whose representatives tend to come from ISPs' main European headquarters and are not necessarily considering particular challenges from Latin America.

Digital Security

This evaluation category was first measured by Karisma's 2017 report for Colombia. At that time, América Móvil-Claro, Telefónica-Movistar, AT&T-DirecTV, and EMCALI did not use encryption (HTTPS protocol) on their websites, while Millicom-Tigo, ETB, and Telebucaramanga already did. Through encryption, HTTPS protects the transmission of personal details users enter on ISPs' websites and apps when checking their accounts, interacting with the company, or purchasing services. IPANDETEC's first report for Panamá in 2019 found that Claro did not use the security protocol on the ISP's virtual customer service channel. Following editions in Perú, Colombia, and Panamá showed that all evaluated companies now use the security protocol. In Perú, Hiperderecho indicates that all featured ISPs also offer users additional security methods, like two-factor authentication for accessing their accounts on ISPs' communication channels. Yet, there are still many gaps when we look at telecom companies' public stance regarding data breaches or what information companies publish about their cybersecurity protocols and measures. Depending on the country, some major telecom companies like Millicom-Tigo, Telefónica-Movistar, and América Móvil-Claro, provide guidance on digital security to users. As for protocols and commitments regarding personal data breaches, QDTD reports in Brazil, Colombia, and Panamá show ISPs making information available at varying degrees and, in Brazil, providing poor public responses to complaints of data breaches.

⇨ See more about data breach-related protocols and commitments in **Section 3.3**.

1.3. The COVID-19 Pandemic Reflected in QDTD Reports

The global health and social emergency created by the COVID-19 pandemic prompted governments to tackle the massive spread of the virus. Hasty technology-based responses raised many serious concerns by experts and civil society advocates working on the intersection of technology and human rights. QDTD reports published during this period have reflected some of these issues in their parameters. For example, emergency regulations threatening network neutrality in Colombia led Karisma to include related criteria in its 2021 report (see Annex).

On the privacy front, government access to user data for COVID-19 control policies stood out among QDTD editions.

Brazil's 2020 report checked which ISPs took a public stance to defend privacy and data protection against government pressure to access telecom data during the pandemic. InternetLab underlined that Oi publicly committed to require the country's national statistics agency, IBGE, to sign a term of responsibility before giving it access to user data due to a regulation later overturned by Brazil's Supreme Court. The report also pointed out that telecom providers have signed data-sharing agreements with states and municipalities. Although government officials disclosed in the press the existence of such agreements, their content was not publicly available. Vivo and Tim publicly committed that only anonymous and aggregated data, via heat maps and pivot tables, would be shared with the government. And after a court in São Paulo ruled this agreement should be public, many telecom providers published the relevant policies on their sites, including TIM, Telefónica-Vivo, América Móvil-Claro, and Oi. However, the companies' policies did not specify the security practices and techniques adopted to ensure the shared data's anonymity. Moreover, ISPs should have published their policies proactively and immediately, and not after public pressure.

This is what Chile's report seeks to foster in more recent editions. Since 2021, Derechos Digitales' QDTD reports spot which providers went public about their data-sharing agreements with public and private institutions. Considering both the COVID-19 pandemic and law enforcement demands in the context of social protests across the country in 2019, Chile's reports began to check which ISPs publicly commit to only hand user sensitive information, like location data, to authorities if requests refer to specific persons and come with previous judicial authorization. Transparency reports should also indicate whether requests target individuals or groups of people (e.g. cell tower searches). When it comes to data-sharing for public policy purposes, ISPs must commit to share only anonymized and aggregate location data with government authorities.

Results in Chile's reports show significant progress. By 2022, Telefónica-Movistar and Entel have published details on their data-sharing agreements to tackle the pandemic. América Móvil-Claro, VTR, and WOM started to report on collective requests the ISPs received from authorities. All featured companies, except Telefónica-Movistar and GTD, committed to require a judicial order and the indication, or individualization, of persons affected in government requests that involve sensitive information. And all ISPs, except GTD and VTR, endorsed the commitment to share only anonymized and aggregate location data for policy purposes.

Finally, Eticas' 2022 report created a particular score to indicate whether ISPs went public with any specific data protection measure related to the pandemic. Of six evaluated telecom companies, only Vodafone received credit for publishing a specific data protection policy on its collaboration with government authorities in COVID-19 control actions. Vodafone's policy commits to important safeguards, such as only sharing aggregate and anonymized data and respecting principles of proportionality and purpose limitation. Although the report mentions the ISP has put adequate security measures in place, it fails to provide any other details on what these measures are. Still, Vodafone goes a step further than other telecom companies in Spain by having made available a specific policy for COVID-related actions.

1.4. Regional Comparison of Major Featured Companies

This section outlines a regional comparison of major telecom companies with operations in Latin America and Spain covered in QDTD reports of at least two different countries. There have been relevant changes in companies' affiliations and geographical distribution over the project years. This is especially true for Central America, where we published editions for Panamá and Nicaragua. Therefore, the market distribution of each company in QDTD reports we indicate below considers the latest edition of each country.

Except for transparency reports, the comparison in this section does not take *global* policies or guidelines into account.

Telefónica/Movistar/Vivo *Operations in Argentina, Brazil, Chile, Colombia, Mexico, Peru, and Spain*	
Data Protection/Privacy Policies	"Privacy and/or Transparency Centers" in all researched countries: Argentina, Brazil, Chile, Colombia, Mexico, Perú, and Spain
Transparency Reports	Global report with detailed information provided for all countries (only recently published in Portuguese). Available on all local websites.
Prior Judicial Authorization	○ Content/Interception: Argentina, Brazil, Chile, Mexico, Peru, Spain ○ Metadata: Brazil, Peru
User Notification	○ General declaration reserving the possibility: Argentina (2019) ○ Denying user notification: Chile, Peru
Law Enforcement Guidelines	Argentina, Brazil, Chile, Colombia, México, Perú. LE guidelines published on Argentina's and México's websites are less informative than those available in the other branches' web pages.

América Móvil/Claro/NET *Operations in Argentina, Brazil, Chile, Colombia, Nicaragua, Panama, Paraguay, and Peru*	
Data Protection/Privacy Policies	○ "Privacy and/or Data Protection Portal": Brazil, Chile ○ Standard policy covering the provision of telecom services: Argentina, Colombia, Paraguay, Perú ○ Standard policy covering only communication channels: Nicaragua ○ Confusing regarding its scope: Panamá
Transparency Reports	○ Local report with aggregate data of government requests: Chile, Perú. In Brazil, Claro provides data in the ISP's sustainability report ○ Global report with aggregate data of government requests: Published as of 2021, it provides aggregate data *per region*. It covers all countries. Regions split into: North America and the Caribbean, Central America, Southern Cone, and Andean Region. Not available on local websites.
Prior Judicial Authorization	○ Content/Interception: Argentina, Brazil, Chile, Perú. ○ Metadata: Brazil, Chile, Perú.
User Notification	○ General declaration reserving the possibility: Chile ○ Commitment to notify in non-criminal cases: Chile, Perú ○ Denying user notification: Panamá
Law Enforcement Guidelines	○ Law Enforcement Guidelines: Chile, Perú ○ Global report: América Móvil's 2021 transparency report includes some information about the procedure followed and applicable law.

Millicom/Tigo *Operations in Colombia, Nicaragua, Paraguay, Panama*	
Data Protection/Privacy Policies	○ No Privacy Center or Portal, except for something similar in Colombia. ○ Confusing regarding its scope: Nicaragua, Panamá, Paraguay
Transparency Reports	○ Local report with aggregate data of government requests: Colombia ○ Global report with aggregate data of government requests: It provides aggregate data *per region*, covering all countries. Regions split into: South America, Central America. Not available on local websites.
Prior Judicial Authorization	○ Content/Interception: Paraguay, Panama ○ Metadata: None
User Notification	○ General declaration reserving the possibility: None ○ Commitment to notify in non-criminal cases: None
Law Enforcement Guidelines	○ Colombia

Other ISPs with presence in more than one country[6]

AT&T/DirecTV (Argentina, Colombia, México), Liberty Latin America (VTR Chile, +Móvil Panamá), Entel (Chile, Perú), Telecom Group (Personal Argentina and Paraguay)

Data Protection/Privacy Policies	○ "Privacy and/or Data Protection Portal" (obs: AT&T has one Privacy Center only in its global website) Entel Chile ○ Standard policy covering the provision of telecom services: AT&T México, DirectTV (Argentina), DirecTV (Colombia), VTR Chile, +Móvil Panamá, Entel Peru, Personal Argentina ○ Standard policy covering only communication channels: Personal Paraguay
Transparency Reports	○ Local report with aggregate data of government requests: VTR Chile, Entel Chile ○ Global report with aggregate data of government requests: AT&T México, DirecTV (Argentina and Colombia). AT&T's report provides very little data for Latin American countries, except for México.
Prior Judicial Authorization	○ Content/Interception: AT&T Mexico, VTR Chile, Entel Chile, Personal Argentina ○ Metadata: AT&T Mexico, VTR Chile, Entel Chile, Personal Argentina
User Notification	○ General declaration reserving the right or possibility: DirectTV Colombia and Argentina, VTR Chile, +Móvil Panamá ○ Explaining limitation and committing to asses circumstances: Entel Chile ○ Commitment to notify in non-criminal cases: none ○ Denying user notification: none
Law Enforcement Guidelines	○ Local report: VTR Chile, Entel Chile

[6] AT&T and Liberty Latin America provide services in other project's countries but we list below only countries that feature the ISPs in their latest published reports.

QDTD reports have also played an important role by encouraging nondominant companies to beat major market leaders in their commitments to transparency and users' privacy. WOM and VTR in Chile are good examples. Moreover, Somos Conexión in Spain, TIM in Brazil, and IPLAN in Argentina have shown that engaging with QDTD reports results in stronger user protections and higher marks over the project's editions.

2. The Application of Human Rights Standards to Communications Surveillance: Government Access to Data and Challenges to ISPs' Best Practices

International human rights law provides the universal framework against which any interference in privacy rights must be assessed. Universal and regional human rights bodies, international courts, and civil society experts and advocates have developed a pivotal and ongoing body of work grounded in international human rights standards on how to protect the right to privacy in the digital age.[7] International human rights instruments make clear that all restrictions to the right to privacy, including the right to be free from arbitrary interference with communications, must follow a three-part test: restrictions must be clearly and accessibly prescribed by law, suitable and necessary to achieve a legitimate aim in a democratic society, and proportionate to the aim pursued.

QDTD reports help shed light on trending threats to the application of human rights standards to government surveillance. These threats endanger necessary and proportionate principles, as well as procedural safeguards and oversight measures required to prevent arbitrary government access to data and uphold the tenets of democratic societies.

Although companies bear responsibility for respecting privacy and mitigating human rights risks in their activities,[8] we must also address the challenges arising from local legislation, law enforcement practices based on interpretations of domestic rules, and worrying patterns in case law. The following sections briefly describe these trending threats and challenges, and analyze how they undermine human rights principles and safeguards.

[7] Electronic Frontier Foundation and ARTICLE19, Necessary & Proportionate Global Legal Analysis, (May 2014). https://necessaryandproportionate.org/global-legal-analysis/; UN General Assembly Resolution on the Right to Privacy in the Digital Age, UN Doc A/RES/75/176 (16 December 2020); UN General Assembly Resolution on Terrorism and Human Rights, UN Doc A/RES/74/147 (18 December 2019); UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/42/15 (7 October 2019); Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/report/4780/pis-guide-international-law-and-surveillance

[8] UN Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011, https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

2.1. Authorized by Law, Necessary, and Proportionate

The OHCHR emphasized that all types of State surveillance-related activities must be conducted on the basis of the law. Such laws need to be sufficiently precise and describe the category of persons that may be subject to surveillance. The High Commissioner pointed out that "surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be sufficiently targeted." QDTD reports flag at least two major points of attention regarding the three-part test that restrictions to privacy must pass to be legitimate under international human rights law. We outline them below.

Nontargeted user data requests or data-sharing agreements for criminal investigation, inspection, or policy purposes

Government authorities' access to large portions of information from unspecified users held by ISPs raise concerns, whether the data is to be used for law enforcement or policy purposes. The intense recourse to surveillance measures in the fight against the COVID-19 pandemic brought these two lines of concern closer together, although the way to assess and address each one has their particularities.

The three-part test for restricting data privacy rights is again the baseline for any government policy involving data processing affecting persons and/or groups. This baseline should include robust nondiscrimination[9] 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, or community control, over whether data-intense policies are legitimate, necessary, and efficient. The baseline should also consider *if* and *how* these policies should be conceived, implemented, or maintained.

That said, we focus on the issue of nontargeted requests for law enforcement purposes.

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.

[9] The Vienna Declaration and Programme of Action note, "The administration of justice, including law enforcement [...] agencies, [...] in full conformity with applicable standards contained in international human rights instruments, [is] essential to the full and non-discriminatory realization of human rights and indispensable to the process of democracy and sustainable development. Vienna Declaration and Programme of Action, World Conference on Human Rights in Vienna, 1993, https://www.ohchr.org/en/instruments-mechanisms/instruments/vienna-declaration-and-programme-action

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. As stressed by the Inter-American Commission on Human Rights (IACHR) Special Rapporteur for Freedom of Expression, "mass surveillance of communications is under no circumstances proportional." In this same vein, the UN High Commissioner 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.

Reverse searches, then, deserve careful attention from human rights courts and bodies, since they twist procedural safeguards and fail to adhere to standards of necessity and proportionality. ISPs should challenge indiscriminate requests for user data and communications. In turn, national courts should uphold international human rights standards and constitutional safeguards by putting a stop to suspicionless searches.

Direct Access

Direct access to telecommunications companies' networks for intercepting communications or obtaining communications-related data is another problematic government surveillance practice reflected in QDTD reports, particularly Colombia's 2021 and 2022 editions (see section 1.2). 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 OHCHR and the European Court of Human Rights stated that direct access practices are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards. Regarding countries covered by QDTD reports, 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, 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 we can underline here. 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. Companies should keep shedding light on those requirements and raising awareness about direct access' inherent risks.

2.2. Judicial Oversight

In furthering standards for the protection of privacy in the digital age, the UN High Commissioner for Human Rights asserted that:

> *[s]urveillance measures, including communications data requests to business enterprises and intelligence-sharing, should be authorized, reviewed and supervised by independent bodies at all stages [...]. The independent body authorizing particular surveillance measures, preferably a judicial authority, needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary and proportionate and authorize (or reject) ex ante the surveillance measures."*

Human rights bodies and experts have repeatedly stated that independent judicial authorities are most suited to authorize communication surveillance measures, and authorization must be *ex ante*—before the surveillance measure takes place. The EU Court of Justice held that the public prosecutor's office, "whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings," cannot be regarded as an *independent* administrative authority to authorize government access to communications data in criminal investigations.

Nonetheless, local legislation or national settled case law in Latin American countries impose challenges for ISPs to require a judicial order before handing communications data to authorities (see section 1.2). In Colombia, the interception of private communications is subject only to subsequent judicial oversight. The Office of the Attorney General has the power to order the interception and proceed with it before a judge assesses the validity of the measure.

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 Perú, recent changes to Legislative Decree 1182 authorized the specialized police investigation unit to request from telecom operators access to real-time cell phone or electronic device location data without a previous judicial order beyond emergency cases when there is an imminent risk or danger to human life and physical integrity. 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. The legal framework in Panamá and Perú, however, requires a prior judicial order for intercepting the content of private communications.

Despite growing understanding among human rights bodies and international courts that communications metadata can be as revealing and intrusive as the content of communications, domestic laws in Latin America still treat metadata as less worthy of protection. "Metadata," such as the identification of parties engaged in communication, IP addresses, locations, the time and duration of communications, and device identifiers, can reveal people's activities, where they live, their relationships, habits, and other details of their lives and everyday routines. Often, national courts also fail to update fundamental rights protections to keep in step with technological changes.

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. About one year before Paraguay's ruling, the Inter-American Court of Human Rights (IA Court) recognized that the protection of communications privacy in the American Convention on Human Rights applied both to content and metadata:

> *Article 11 applies to telephone conversations irrespective of their content and can even include both the technical operations designed to record this content [...], or any other element of the communication process; for example, the destination or origin of the calls that are made, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to record the content of the call [...]. In brief, the protection of privacy is manifested in the right that individuals other than those conversing may not illegally obtain information on the content of the telephone conversations or other aspects inherent in the communication process, such as those mentioned.*

The IA Court stated that the "fluidity of information places the individual's right to privacy at greater risk owing to the new technological tools and their increased use." As such, "the State must increase its commitment to adapt the traditional forms of protecting the right to privacy to current times." Domestic laws and courts in Latin American countries must respond to the IA Court's call to properly update the protection granted to data privacy. It is worth noting that in many Latin American countries the American Convention on Human Rights holds the same or even higher status than countries' own national constitutions. Therefore, companies, among others, can explore strategic litigation to reinforce privacy safeguards before weak local standards. On the

other hand, lawmakers and courts should not wait to level up protections against increasingly pervasive and intrusive surveillance capabilities.

2.3. Transparency

Secret laws are not laws. Under international human rights standards, a law is only a legitimate and valid basis to authorize the restriction of privacy and other rights if it is publicly accessible. As stressed by the OHCHR when addressing the right to privacy in the digital age, "secret rules and secret interpretations of law do not have the necessary qualities of 'law." The IACHR Special Rapporteur for Freedom of Expression pointed out that States should disclose procedures for government surveillance. The minimum range of information that should be made public includes procedures for authorizing surveillance, selecting targets, and handling collected data, as well as the protocols for sharing, storing, and destroying the data.

Yet, more often than not law enforcement protocols for surveillance are 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 LD 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. Government surveillance techniques should be subject to public scrutiny and independent oversight to ensure that procedures respect human rights and proper checks are in place. ISPs' public law enforcement guidelines help shed light on such procedures, but the regulations they follow should also be publicly accessible.

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.

2.4. User Notification and Right to Remedy

Notifying users when governments are seeking their information from service providers is essential to curb improper requests and protect privacy and due process rights. User notification enables people to plan for a legal defense and challenge potentially arbitrary requests. Before the revolution in electronic communication, police seeking people's information had to knock on their door and show a warrant. The person searched could observe whether the police searched or seized their written correspondence, and if they felt the intrusion was improper, ask a court to intervene.

Electronic surveillance, on the other hand, is much more surreptitious. A person's data can be intercepted or acquired directly from telecom or internet providers and the person is not aware unless or until the data is used as evidence leading to criminal charges. As a result, people are least likely to discover the violation of their privacy rights. International courts have recognized the importance of notifying persons subject to surveillance. The European Court of Human Rights has held that notice is:

> *[...] inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle*

> *little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively."*

Similarly, the EU Court of Justice has emphasized that "the competent national authorities to whom access to the retained data has been granted must notify the persons affected [...] as soon as that notification is no longer liable to jeopardize the investigations being undertaken by those authorities." The UN High Commissioner for Human Rights also recognized that users who have been subject to surveillance should be notified after the measure.

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. QDTD 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.

Secrecy over the interception of communications provided by law must be time limited and not extended automatically to other surveillance measures, like access to stored communications data. When not clearly established by law, delaying notification of affected users should be justified to a court and tied to an actual danger to the investigation or harm to a person. State authorities and companies should not interpret legal safeguards preserving confidentiality of user data retained or captured by ISPs and delivered to authorities to justify blocking user notification. IPANDETEC's 2021 edition shows the flaws of such an interpretation, used by companies in the latest Panamá report. While data collected through surveillance is restricted from being disclosed to nonauthorized third parties, when the data pertains to users, its collection and contents should not be kept secret from those users. Traditional access, rectification, cancellation, and opposition (ARCO) rights in Latin American data protection frameworks, especially when backed by a constitutional right, reinforce the person's right to know that his or her personal information was shared with government authorities also in the context of law enforcement.

2.5. Policy Commitment and Impact Assessments

The UN Guiding Principles on Business and Human Rights (UN Guiding Principles) provide a principled approach for all companies to prevent, mitigate, and address adverse impacts on human rights related to their activities. The operational principles highlight that companies have a responsibility to respect human rights, which includes making a policy commitment to respect human rights, conduct human rights due diligence, and provide or cooperate in remediation of abuse in cases where the company has caused or contributed to adverse impacts to human rights.

Keeping this in mind, ADC's latest report for Argentina assessed which ISPs have clear public policy commitments to respect human rights. Out of six evaluated companies, only IPLAN and Telefónica-Movistar received credit for having made any public statement in that regard. Movistar's policies are far more comprehensive than IPLAN's. In addition, Movistar has also devised and published a Personal Data Protection Governance Model, primarily based on the compliance with the EU GDPR. ADC's report also identified which telecom companies carry out privacy and data protection impact assessments, and whether they disclose assessment results and/or related mitigation

measures they adopted. Telefónica-Movistar was the only company that reported on how it periodically conducts impact assessments as part of its human rights due diligence.

Yet, Telefónica's Brazilian subsidiary, Vivo, has failed to draft and publish a data protection impact assessment (DPIA) for its operations in Brazil, at least until the release of InternetLab's 2022 report. The company was not alone. InternetLab's researchers did not find DPIAs available for any of the evaluated companies, although the ISP Oi reported having conducted its first assessment in 2021. Brazil's Data Protection Authority recommends data controllers conduct DPIAs in any context where personal data processing operations could create a high risk to ensuring data protection principles and the data subject's civil liberties and fundamental rights. It also recommends data controllers make DPIAs publicly accessible in line with data protection principles in Brazilian law. As such, telecom companies should take up the commitment to assessing and addressing adverse impacts of their business activities—as well as reporting about findings and measures adopted—within their responsibility to respect human rights. Accordingly, the Brazilian association of telecom providers Conexis released a Code of Good Practice in Data Protection that elaborates on steps telecom companies should follow when conducting their DPIAs. Transparency and stakeholders' engagement, including with users, are crucial to ensure that adverse impacts are properly identified, analyzed, and mitigated on an ongoing basis.

Data protection frameworks play a relevant role in criteria partners evaluate across QDTD reports. The next section goes deeper into companies' policies and practices vis-à-vis data protection principles and safeguards.

3. Data Protection Frameworks: Advances and Shortcomings

Several Latin American countries have enacted data protection laws. Chile and Argentina first approved their data protection frameworks more than two decades ago, and are now debating updates to the legislation. In a recent wave inspired by the EU's GDPR, countries like Brazil, Panamá, and Ecuador finally adopted comprehensive data protection laws. Others, such as Paraguay, have draft bills pending in Congress and still lack a comprehensive regime to regulate the processing of personal data.

In many jurisdictions in the region, data protection legislation does not apply to intelligence and law enforcement agencies. As a result, critical safeguards provided by data protection regulations are not included in rules these agencies must follow when processing personal information. This is a gap that Latin American jurisdictions must address to properly protect data privacy and the myriad of rights it upholds. Yet, such gaps do not diminish ISPs' responsibilities to comply with their duties before data protection laws, including when responding to law enforcement requests for user data.

While the previous section focused on companies' collaboration with government authorities, the following section will consider data protection principles and safeguards to highlight strides ISPs made over QDTD reports and weaknesses they still have to overcome.

3.1. Data Protection Policies

Transparency is directly linked to ensuring fair personal data processing. Checking whether ISPs provide easily accessible and understandable information beforehand on which data they collect from users, and why and how such data is processed, has been a shared parameter across QDTD reports since early editions.

As noted in Section 1.2, the presence of data protection laws in some of the researched countries did not necessarily mean that these policies were readily available and easy to locate in their first editions. In Colombia, only one ISP received full credit in this category in Karisma's 2015 report. In Chile, no more than two companies did so in Derechos Digitales' 2017 report. IPANDETEC's latest reports show how finding data protection policies in ISPs' local websites covering companies' provision of internet and telecommunications services remains a challenge in Panamá and Nicarágua.

Over the years, QDTD reports have increased the detail of information partners look for in ISPs' contracts and data protection policies. On the bright side, overall scores for this category have improved across editions even with stricter requirements as publishing such policies became more widespread among service providers. However, in many cases companies still fall short of providing basic information about user personal data processing. We provide some general highlights below.

Purpose of the processing

The contrast between first and last editions in regard to ISPs' disclosure of the purpose of personal data processing is noteworthy. For instance, while only one Brazilian ISP did so in InternetLab's 2016 report, all featured ISPs in the 2022 edition received at least a partial credit for disclosing that information. Yet, advances can be slower in specific local contexts. In TEDIC's 2022 edition for Paraguay, for example, three out of five companies still failed to explain the purposes for processing user data. In fact, Personal and VOX-Hola Paraguay did not even have data protection policies easily accessible on their websites. Moreover, the level of detail, and whether companies go beyond vague purposes descriptions, such as "to provide services" or "to improve user experience" is highly variable among QDTD countries.

Even reports in places with a strong data protection background underscored generic purpose formulations, such as Eticas' 2018 edition for Spain. In turn, América Móvil-Claro stands out in some QDTD countries for providing a nice table (Chile) or a detailed webpage (Brazil) matching types of data collected and related purposes. Yet, the company provides comprehensive, but less user-friendly information in Argentina and Panamá, and a much less thorough description in Paraguay. In Brazil, the company Oi organized its data protection policy with graphics and visual aids to make information easier to understand, including details about data processing of noncustomers.

Finally, user data processing for advertising and personalization of commercial offers is quite often informed as an authorized purpose across ISPs' policies, although it goes beyond what is needed for the regular provision of internet and telecommunications services. As such, companies should provide a separate opportunity for consent, or at minimum, make clear to users how they can opt-out of advertising purposes.

Information about storing user personal data

Another basic information that companies should easily provide in their data protection policy pertains to whether and for how long they store or retain user data. Companies committed to transparency and data minimization should be clear about which type of user data they keep in their databases and respective storage times considering legal obligations and purposes of processing. Although we also see improvements here over QDTD editions, it is striking that ISPs still need a push to properly disclose that information. For example, all companies featured in Paraguay's and Panamá's latest reports failed to do so. Regarding Panamá, IPANDETEC explains that both Más Móvil's and Digicel's policies mentioned they retain user data but did not specify the length of the retention. Four out of nine ISPs evaluated in Colombia, half of them in Chile, and most of them in Perú, Spain, and Brazil, at least partially informed about user data retention or storage. QDTD partners in Chile and Brazil have also checked if companies disclose in which circumstances or how they delete user data, which is a piece of information even more difficult to find in companies' policies.

Data-sharing with third parties

Many QDTD reports evaluate whether ISPs provide information about sharing user data with third parties. Often companies' policies include broad mentions to the possibility of sharing data with government authorities, sometimes specifying them, and commercial partners.

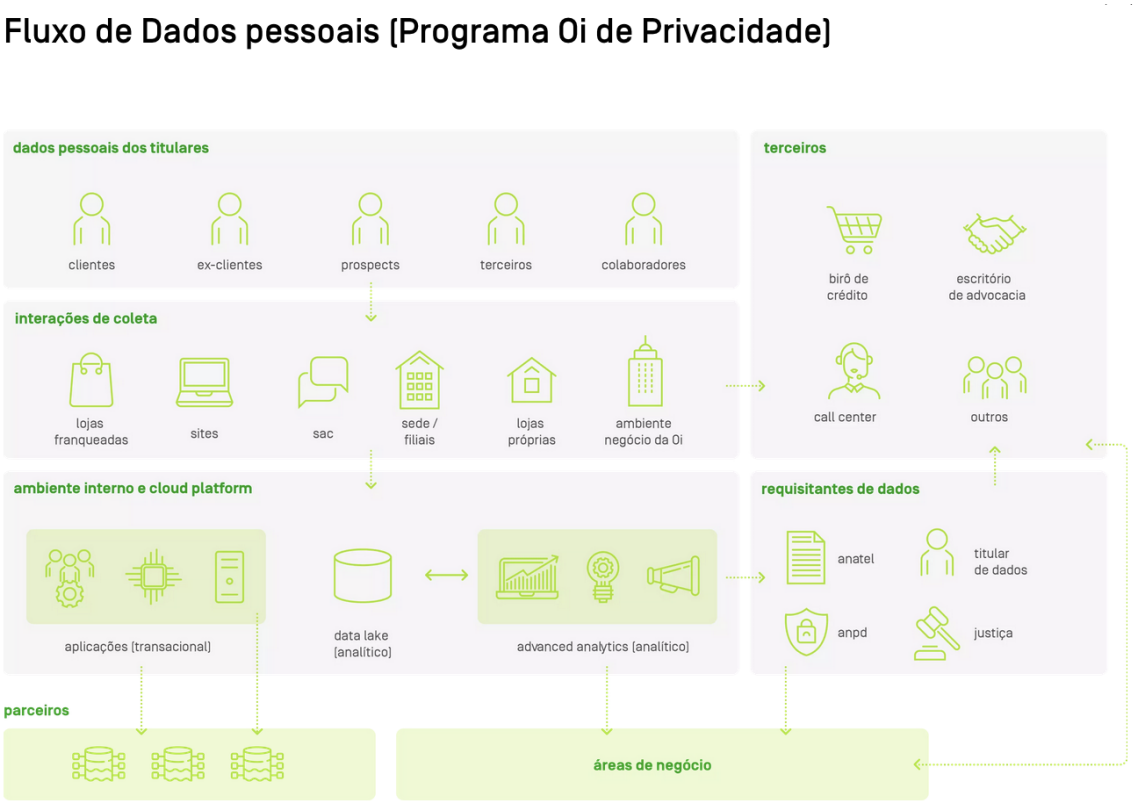
Paraguay's 2022 report highlights also the opposite—companies that state not sharing user data without consent, except when required by law or by a judge. Copaco establishes it will not sell, give or distribute the personal information it collects without user consent, unless required by a judge with a court order. The policy itself does not include any standard and previous consent in that sense. However, TEDIC underlines that the policy made available in Copaco's website refers only to the data the ISP collects from the use of its apps, and does not cover its general provision of internet and telecommunications services.

A similar commitment is found in Personal's policy. Yet, as TEDIC points out, the same policy states that customers' personal information is used by *Club Personal* to provide and improve benefits and offers of mobile services, and may be used for promotional marketing and/or statistical purposes. There's no further information on what *Club Personal* means and whether it comprises other companies or partners. In Chile's 2022 report, Derechos Digitales rails at VTR because of a clause in the ISP's policy setting that the user, at the moment of contracting VTR's services, tacitly authorizes third parties to access user contact data, contracted services, and/or payment behavior.

This kind of surreptitious clauses that seek to underpin blanket and tacit "authorizations" for sharing user data with third parties run afoul of the tenets of a fair personal data processing and undermine user consent and self-determination as key elements of data protection. Companies should abandon deceptive methods, and clauses such as these should not be considered valid. If data sharing is needed due to the complexity of companies' operations, regarding data storage, customer service, among others, this should be clearer and not mixed with other purposes that are not essential to the provision of services, like advertising.

Finally, Brazil's 2022 report increased the details checked in companies' policies for this topic. InternetLab assessed if ISPs inform which kind of collaborators or third parties

have access to user data, and the purposes for sharing data. Researchers also looked if ISPs commit to assess third-parties' compliance with data protection rules. Half of the companies met all the parameters, that is Claro/NET, Oi, and TIM. Claro/NET breaks down the list with whom it shares user data and why (see title *Compartilhamento de dados*). When requested by the user, Claro/NET also details the name of each third party with which the company shares data. TIM and Oi provide a summarized list of third-parties categories. TIM details them according to the purpose of the sharing, as follows: "technology services", "performance analysis", "market research", and "to safeguard and protect TIM's rights". Oi discloses the type of third-parties:"commercial and sales partners", "billing offices and/or agencies", "law firms", "call center services", and government authorities. Interestingly, the ISP has made available a chart describing the flow of user personal data (below, in Portuguese):



International data transfers

Relatedly, some QDTD reports verify if companies mention in their contracts or policies whether they conduct international transfers of users' personal data. This is important because the jurisdiction in which the data is stored or processed affects the legal regime of rules and protections applied to the use and access of user data by government authorities and private parties. Data protection laws in many countries include rules regarding the international transfer of personal data. These rules aim to ensure an adequate level of protection for individuals' right to data protection in the recipient country. Such protection includes appropriate safeguards and effective legal remedies to enforce data protection rights. Essentially, the legal regime of rules and protections applied to the use and access of user data by government authorities and private parties

in the recipient country must align with the data protection rules in the country where the data originated.

Companies' policies providing information about whether, when, and why these international transfers take place is the initial step for assessing if they duly protect users' rights regardless of borders. QDTD reports' results are mixed, although most of the companies assessed in Brazil's, Chile's, and Spain's latest studies mention they share or may share user data abroad.

At least in Brazil's report, such mentions are for the most part related with using cloud services to store user data. TIM gives other examples, such as providing international roaming services, or "when it contracts any relevant supplier for the ISP to provide its services that needs to process user personal data abroad"—which is a very generic explanation in terms of types of providers and circumstances in which an international transfer is needed. TIM also clarifies that cloud service providers may at any time change the location where they host user data but the ISP seeks to contractually limit these transfers so they occur safely and to countries with laws that ensure adequate levels of security and data protection. The main third-party servers used by TIM are located in Brazil, the European Economic Area (EEA), and California, in the US.

In turn, Algar does not specify the instances it may transfer user personal data abroad (beyond listing hypotheses for international data transfers set in Brazil's data protection law), or where foreign servers used by the company are located. Yet, Algar declares that the company's Data Protection Officer (DPO) must assess any international data sharing to ascertain whether the destination country has an adequate level of data protection compared to Brazil's legal system. The transfer may also occur when the receiving controller follows mechanisms like standard contractual clauses and global corporate standards.

In Spain, Eticas' 2022 report checked not only if companies provided general information about international data transfers, but also if they asked for user explicit consent or offered users to opt-out to such transfers. Only four ISPs out of 15 assessed companies, including telecom providers, home sales and rental sites, and apps for selling second-hand goods, received full credit for this parameter.

3.2. Data Subject's Rights

Another important portion of companies' policies relates to informing users about their rights and the mechanisms the company puts in place for users to exercise those rights. Regardless of differences among data protection legal frameworks, a traditional set of data rights in the region comprises the often-called ARCO rights (access, rectification, cancellation, and opposition). Some QDTD reports have evaluated the information ISPs provide to users on that front, and a couple of them have tested ISPs' response to users' requests to access their personal data. Here we summarize the main findings.

Providing information

Since its first edition for Argentina in 2018, ADC has been checking if ISPs identify data subject's rights in their policies. At the time, Telecentro failed to do so and IPLAN and Telecom (Arnet) mentioned ARCO rights, but only vaguely, enunciating the rights without further explanation. What's worse, Telecom (Arnet) required those seeking access to personal data to physically mail a letter with a notarized signature. Besides

adding red tape, the requirement goes against a principle in Argentina's data protection law that users shouldn't be charged to get access to their personal data. In ADC's 2022 report, all evaluated companies inform users about their data subject's rights. But there are still ups and downs. This time, Arlink is the company that requires a notarized letter to give users access to their personal data. Claro provides a form, which is not easily accessible through the local company website and, according to ADC, requires an excessive amount of user data compared to what is stipulated in Argentina's data protection law. On the upside, IPLAN offers a detailed explanation on how users can exercise their ARCO rights and provides a standard form users can send by mail or email to gain access to their personal data. The form includes recordings from surveillance cameras IPLAN uses in its facilities.

The first time InternetLab assessed this parameter was in Brazil's 2019 edition. Contrary to Argentina, back then only Telefónica-Vivo received full credit for detailing users' ARCO rights and ways they could contact Vivo to exercise such rights. Results have significantly improved by the 2022 edition. Five out of six featured ISPs fully complied with this parameter, while Brisanet partially did so. This is because Brisanet informs how users can reach out to the company to claim their rights, but the description it offers about those rights are incomplete and even misleading. InternetLab highlights a clause of the ISP's broadband contract that waives users' privacy safeguards for publicly available data, which disregards protections granted by Brazilian law.

Finally, IPANDETEC included this parameter in Panamá's latest report. Only half of the companies explained ARCO rights and the means to exercise them—Claro and Más Móvil. Yet, while Claro offers various channels users can use for that matter (i.e. Claro's WhatsApp account, call center, or email), those seeking to request access to their personal data from Más Móvil must personally go to the ISP's headquarters. While it's crucial for companies to verify the authenticity of who is requesting access to personal data, users shouldn't have to incur costs or travel. As for the other two featured companies, Digicel does not mention users' ARCO rights and provides an email not specific for Panamá and an US telephone number as point of contact. In turn, Tigo Panamá describes how users can exercise their access and rectification rights, but the policy available on the ISPs' local website was limited to user data collected through the company's apps and websites.

Complying with user's right to access their personal data

This parameter was first evaluated in México's 2016 edition. R3D researchers checked if mobile telecom companies properly responded to access to data requests. That is, if before a user request, the mobile provider handed the user his or her personal data, including communications metadata like call records and location data, in an electronic format and within the 20-day deadline set in Mexico's data protection law. All three featured companies failed. AT&T, Telefónica-Movistar, and América Móvil-Telcel left R3D researchers without a response to their request even after the organization petitioned to Mexico's data protection authority (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) to confirm that communications metadata is personal data, and that telecom companies had the obligation to hand them to users who filed access to data requests.

More recently, InternetLab started checking whether Brazilian ISPs timely respond to users' requests either to confirm if the company processes their personal data or to get access to such data, following standards established in Brazil's data protection law. Out of six companies, only Claro/NET and TIM fully complied with this parameter in

InternetLab's 2022 report. However, the data these companies provided was limited to subscriber information and did not include all the user communications metadata that telecom companies regularly process. Algar did reply on time, but to state that the ISP did not process any personal data from the requesting account, which is probably not right as the request came from an Algar's customer. InternetLab researchers were not able to obtain any response from Oi, and could not even file the request for Vivo due to technical problems on the company's app.

Finally, Brisanet did not provide any online channel for noncustomers to confirm whether the company processes their data. Noncustomers may have their personal data processed by a telecom operator, for example, when calling or receiving calls from that operator's customers. They have the same right as customers to confirm whether the company processed their personal data and get access to that data. But Brisanet requires noncustomers to send a physical letter to the company's headquarters with notarized copies of their national ID and signature. Although checking measures are relevant to verify if the data requested pertains to the person making the request, the company should provide an online and less bureaucratic alternative for all users, not only their customers.

3.3. Data Breaches: Protocols and Actions

How companies prevent and address personal data breaches is also a critical component of data privacy concerns. Some QDTD reports have looked at that in greater detail.

Since Colombia's 2017 edition, Karisma assessed which ISPs provided information on how they mitigate data breaches. Back then, just Millicom-Tigo and Telebucaramanga went well in this parameter among seven featured ISPs. As Karisma underlined, the poor results obtained by América Móvil-Claro and Telefónica-Movistar raised a red flag for most of the Colombian users that relied on these companies to secure their personal data. The situation only slightly improved by Karisma's 2022 edition. Telefónica-Movistar and Millicom-Tigo count on a protocol and documentation to mitigate data breaches. Skynet generally discloses what security measures it deploys, but not which contingency measures the ISP applies in case of security breaches. ETB also provides general information on security measures and how it deals with security incidents, but it fails to describe concrete mitigation measures. The other five evaluated companies did not receive any credit for this category.

IPANDETEC first assessed this parameter in Panamá's 2021 report. No company except for Millicom-Tigo had publicly accessible information indicating they adopt a protocol to inform their users about data breaches, even though Panamá's data protection regulation sets a notification duty in such cases (particularly the Executive Decree 235/2021).

However, even Tigo did not provide that information on the ISP's website for Panamá, but only on a Millicom's webpage, in English, about cybersecurity. What's more, the webpage is somewhat ciphered when disclosing the company's security protocols. It states that "Millicom has implemented a risk framework which is based on a combination of the NIST Cybersecurity Framework (CSF) as well as the ISO/IEC 27001:2013." By knowing that such risk frameworks involve best practices to mitigate and address data breaches, which includes internal and public communication about the security incident, IPANDETEC researchers concluded that informing affected users is

part of the protocols Tigo Panamá adopts. Yet, the excerpt we mentioned is far from informative when it comes to users in general.

In Brazil, InternetLab's 2021 report checked which ISPs took a public stance in favor of user security by providing concrete information on risk mitigation strategies and incident prevention. Only Brisanet did not receive credit in this parameter. Highlights included a new document from TIM entitled "Information Security and Cybersecurity Policy," which, among other things, provided a specific communication channel for security cases. But the news wasn't all good. Even though Claro, Oi, and TIM scored well for their public statements regarding cyber risk mitigation, InternetLab pointed out that they all failed to provide robust answers to accusations of data breaches (Claro in 2020, and Oi and TIM in 2021).

The ISPs provided only "generic answers." InternetLab stressed that "no robust explanations about the case were given, nor were any standards or techniques concretely advocated that could address the allegations [of data breach]." Telefónica-Vivo also faced data breach accusations in 2020, receiving notification from consumer and telecom authorities. According to InternetLab, the company sent public responses to authorities, claiming to have evaluated its internal systems and found no security incidents. The responses did not mention any improvements in Vivo's security measures.

3.4. Face recognition

The use of facial recognition is increasing among mobile service providers, especially for prepaid lines, as a method of verification to activate telecommunications services. Face recognition represents an inherent threat to privacy, social justice, free expression, and information security. 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.

QDTD reports started to look closer into ISPs' use of this technology with Brazil's latest edition. Unfortunately, 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. Oi has also shared with InternetLab's researchers statements the company issued that underline the importance of carrying out impact assessments when public bodies contract with service providers of facial recognition technology.

4. Conclusions and Recommendations

The overview of achievements, challenges, and trends throughout the series of QDTD reports underlines an important set of conclusions.

Data Protection Policies and Practices

Despite great progress, the presence of data protection laws in force still does not correspond necessarily to companies' data privacy policies that are comprehensive and easy to find and understand. What's worse, it does not necessarily lead to ISPs making available data privacy policies that apply to the provision of telecommunications services instead of only to the collection of user data through their websites and apps. This is a challenge particularly in smaller markets, like Panamá, Nicaragua, and Paraguay, which major telecom companies seem to deprioritize, at least in the aspects QDTD reports evaluate. In the case of Paraguay, there is no comprehensive data protection legislation yet. In fact, the enforcement hurdles of data protection frameworks in the region do not diminish the importance of having such laws. Three main concerns arise in this regard: Latin American countries that still lack comprehensive data protection laws or rely on outdated ones, the exclusion of law enforcement and intelligence agencies from the scope of several data protection laws in the region, and legislations that fail to ensure effective oversight powers and structure to data protection authorities.

As for companies' policies recently assessed in QDTD reports, telecom providers still fall short of providing sufficient details about basic information on how they process user data. Among other gaps, many of their policies show only generic statements about the purposes for processing user personal data, are silent or say very little about their data breach protocols, and lack meaningful information about data storage times and data deletion procedures, as well as about data-sharing with third parties (including when they involve international data transfers). Besides, there is ISPs' problematic practice of mentioning they share user data with third parties as it could work as a blanket and covert authorization for the transfer of user data to commercial partners with no specific opportunity for users to know about this or consent. While telecom companies usually do better informing users about their data subject's rights and the means to exercise them, they still fall short of ensuring users can access their data in an effective and practical way.

Transparency Reports and Law Enforcement Guidelines

Transparency reports are both an industry norm and a persistent challenge. Most or half of the ISPs in countries like Spain, Panamá, Paraguay, Perú, and Colombia still do not disclose detailed statistical information about government requests for user data. América Móvil's and Millicom's global reports do not provide statistical information per country. Both companies have few subsidiaries that publish local, country-specific,

transparency reports. AT&T's report shows a significant imbalance in what it discloses about the countries where it operates. It shares way more information about government demands in the US, although it also provides some detailing on law enforcement requests in México. For all the other countries, the information AT&T's report provides is minimal. Telefónica is the ISP that best balances the data it publishes for all countries where it provides services, while Millicom stands out for its qualitative reporting. With few exceptions, global transparency reports are not easily available on telecom companies' local websites.

Likewise, there is an increasing trend to consolidate the disclosure of LE guidelines as a best practice. However, the type and detail of disclosed information are highly variable among ISPs and ISPs' local branches. In fact, finding local, country-specific, LE guidelines remains a major challenge. QDTD partners couldn't find any or identified very few of them in Panamá, Paraguay, and Spain. Only major companies publish local LE guidelines in Perú. Global summarized guidelines are not enough to give insight into companies' steps before government data requests as they fail to provide meaningful country-level information about procedures and safeguards local authorities must follow.

Judicial Authorization and User Notification

The margin allowed for stronger safeguards in each domestic legal privacy framework directly impacts telecom companies' commitments to require a judicial order before handing user data to authorities and to notify users about government data demands. National laws that authorize prosecutors or the police to access user metadata without a previous judicial order, beyond emergency circumstances, fail to properly protect users' privacy and data protection rights. Moreover, domestic legislation establishing almost unfettered secrecy provisions in regard to government access to user data poses a very concerning barrier to companies' commitments to notify users about government data requests, which hampers users' right to remedy and our societal ability to control abuses in government surveillance.

Commitments to User Privacy

With few exceptions, this is generally a difficult category to measure in QDTD reports, as it largely depends on publicly streamlined access to case law in countries' lower courts (such as in Brazil) and/or ISPs' engagement with QDTD researchers. Telecom companies do not release their actions before courts, Congress, or policy discussions systematically. While major global ISPs do publish about general policy positions on their parent company's corporate websites, we do not usually find similar content on their local branches' webpages. It is remarkable, then, that Claro Chile created a specific section on its website to report about its interactions with public authorities, and that Oi in Brazil includes information about their judicial challenges to government requests in the company's sustainability report. When QDTD reports succeed in pointing out ISPs' actions against arbitrary regulations or disproportionate government requests, or their

public stance in favor of privacy safeguards, the examples they highlight demonstrate the crucial role ISPs play in limiting surveillance abuses.

This reinforces the importance of telecom companies to conduct data protection impact assessments and undertake human rights due diligence, in a holistic look at their commercial practices and collaboration with government authorities. Regrettably, they still have a long way to go on both fronts. While some major global companies have developed internal procedures to meet these requirements, turning them into a consolidated practice among ISPs is still a challenge. Smaller companies should also take it up as a positive differential in their favor. Finally, it is concerning that telecom companies with a broader presence in Latin America, or their representatives in the region, are by and large out of relevant multi-stakeholder or industry initiatives to foster companies' compliance with human rights.

Worrying Emerging Trends

Over the years, QDTD reports added new parameters to reflect and respond to the emergence of concerning trends. As we discussed in Sections 1.2, 1.3, 2.1, and 3.4, those concerning trends include government mandates to directly access the networks of telecom providers, often without the company's knowledge, to get users' communications data. They also include law enforcement nontargeted, massive, requests (such as reverse location searches), and policy-related indiscriminate requests for user data without proper safeguards (e.g. actions during the outbreak of the COVID pandemic). Finally, we highlight the increasing use of mandatory facial recognition and biometric data collection to activate telecommunications services, especially prepaid mobile lines.

In view of these conclusions and building on the detailed basis set by the Necessary and Proportionate Principles on the Application of Human Rights to Communications Surveillance, we recommend:

Companies

- Publish comprehensive, user-friendly, and country-based information about their data privacy policies and practices throughout the provision of their services, instead of disclosing only the collection of user data from companies' websites and apps. Comprehensive data privacy policies include meaningful information about how they store user data (including the type of data stored, for how long, and what happens after this period), their data-sharing practices with third parties (including a breakdown of third parties involved, purposes of sharing, and a commitment to assess third-parties' compliance with data protection safeguards), international data transfers and their purposes, and company's security measures and data breach protocols, as well as meaningful information about data subject's rights (including how users can effectively exercise such rights).

- Make their policies available in the languages spoken in the country where they provide services, such as native languages. Provide customer service channels capable of offering assistance in those languages to the greatest extent possible.

- Ensure the proper exercise of data subject's rights related to all personal data the company processes, including the right to access personal data, regardless of whether or not the user is one of its customers. The company's responsibility to check the authenticity of the user making the request should not inflict a burden on users with bureaucratic or displacement hurdles. The response to a request to access personal data should cover all data related to that user, including communications metadata and inferred data (in case of user profiling, for example).

- Have policies, procedures, and structure in place to effectively and transparently address data breaches. Consistently report about the company's actions to ensure security and privacy when storing and otherwise processing user data.

- Abandon deceptive methods like including surreptitious clauses in their policies with the aim to broadly "authorize" data sharing with third parties. If data sharing is necessary for companies' regular operations, regarding data storage, customer service, among others, these purposes should be clear in companies' policies, and not mixed with other purposes that are not essential to the provision of services, such as advertising. In such cases, ISPs should provide a separate opportunity for consent, or at minimum, make clear to users how they can opt-out.

- Publicly report and, at the greatest extent possible, be transparent about data-sharing agreements for criminal investigation, inspection, or policy purposes. Shed light on direct access requirements and raise awareness about its inherent risks.

- Publish detailed statistical transparency reports regarding all government access to their customers' data. At a minimum, break down aggregate data per country, type of data (content interception, metadata, and user subscriber information), number of requests approved and rejected, and number of users' accesses affected. Local transparency reports in QDTD studies shows that ISPs can also provide other important aggregate data, such as the number of real-time location requests, number or proportion of targeted *vs* non-targeted (massive) requests, reasons for rejecting government requests, and a breakdown of demands per requesting authority in combination with the type of data requested.

- Do not take legal provisions on the secrecy of private communications and the confidentiality of investigative measures *per se* as a prohibition for publishing transparency reports with country-specific aggregate data about government requests. When government authorities adopt such an interpretation, explore avenues to engage with them towards overcoming strict understandings of the

law or consider ways to challenge in courts such a disproportionate limitation to transparency.

- Publish guidelines for government agencies seeking users' data. It is important for the public to know how police and other government agencies obtain customer data from service providers. To ensure public access to this information, providers should transparently publish the guidelines they provide to government agencies. Either in their transparency report or LE guidelines, companies should include and define what they mean by metadata, clarifying what kind of user data is included in such reported categories. They should also detail, for each country, the applicable legal framework for government access to data and the competent authorities to request each category of user data.

- Adopt most protective interpretations of domestic legal frameworks to require a judicial order before handing over user data to authorities, except in cases of emergency when there is imminent risk of danger to human life (see Principles 6 and 7). Challenge arbitrary or disproportionate government requests for user data, including nontargeted, massive requests, like reverse location searches.

- Notify users about government data requests at the first opportunity allowed by law, including in noncriminal cases (see Principle 8). Engage with government authorities to explore ways to best implement user notification in accordance with domestic legal frameworks. Do not broadly interpret the secrecy over communication interception procedures to automatically cover other surveillance measures, like access to stored communications data. In addition, the confidentiality of user data should not justify limitations on the company to notify the user to whom the data relates, as such confidentiality serves to protect users, not to blindside them before third-parties' requests to their data.

- Assess opportunities for strategic litigation to reinforce privacy safeguards present in constitutional and human rights norms vis-à-vis weak local standards. At the greatest extent possible, engage in local policy and legislative debates advocating for strong privacy and data protection safeguards. Disclose country-specific information about litigation and policy efforts and actions in favor of users' privacy and data protection.

- Adopt clear, comprehensive, and robust policy commitments to respect human rights in the provision of its products and services. Conduct data protection and human rights impact assessments on an ongoing basis, publishing their results and reporting about mitigation measures the company has adopted.

- Engage with multi-stakeholder and industry initiatives committed to uphold privacy, data protection, and freedom of expression in the provision of telecommunications services and internet access. Ensure the participation of companies' representatives that can properly address the Latin American context and its particular challenges.

We understand that many of these recommendations may be challenging for smaller ISPs. While respecting users' human rights, and preventing and mitigating harms, should be regularly integrated into any ISPs' business practices and plans, human rights institutions, data protection authorities, industry associations, and civil society organizations can all play a role in providing guidance and feedback on how companies can achieve that in the most effective way possible.[10] Moreover, all these actors join a broader ecosystem qualified to advocate, both at local and regional levels, for robust privacy and data protection safeguards in the provision of telecommunications and internet services.

States

Any limitation to human rights imposed 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 limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to 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. We have detailed such safeguards throughout the Necessary and Proportionate Principles. The recommendations below articulate this set of principles with QDTD reports' findings. In this sense, States should:

- 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).

- Be cautious about data-sharing agreements with the government for policy or inspection purposes (see Section 2.1). Undertake them only when necessary and

[10] For instance, the OHCHR's B-Tech project provides authoritative guidance and resources for implementing the United Nations Guiding Principles on Business and Human rights in the technology space. Available at: https://www.ohchr.org/en/business-and-human-rights/b-tech-project

proportionate for the achievement of a legitimate aim in a democratic society, and based upon a consistent and democratically approved legal basis. 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. 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.

- 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 (see Principle 8). 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.[11]

- Cease disproportionate surveillance mandates. Governments should not require ISPs and telecom operators to grant direct access to their networks or servers. Indiscriminate, suspicionless searches targeting communications data also fail to meet necessary and proportionate standards (see Section 2.1). 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.

- Abandon facial recognition and other biometric data collection mandates for users' to activate and benefit from telecommunications services.

[11] 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 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.