tigo MILLICOM
THE DIGITAL LIFESTYLE

2019

Millicom Group Law Enforcement Disclosure (LED) Report

We believe in better.
We believe in tigo

What's inside this report...

Contents

1. Introduction

Millicom's 2019 Law Enforcement Disclosure (LED) report summarizes the extent and context of our interactions with law enforcement agencies and governments on issues that affect the privacy or freedom of expression (FoE) of our customers.

Privacy and FoE remain among the most material and relevant topics for companies that provide communications services. In recent years, several high-profile incidents have made these topics increasingly mainstream as people recognize the value of their personal data and privacy online.

Since 2015, Millicom has produced an annual Law Enforcement Disclosure (LED) report in line with our desire to be as transparent as possible with our customers in how we handle government requests for their data, the challenges we face from time to time in dealing with government requests and how we manage such challenges. In this report, we also set out our ongoing commitment and progress in the areas of privacy and FoE, how our operations may impact human rights more generally, and how we work independently and with others to minimize potential negative impacts. We issue this report in both English and Spanish given that our business focus is primarily in located in Latin America.

Our business success relies on customers' trust in us to respect their privacy and freedom of expression, which also goes hand-in-hand with our duty to respect local laws in the countries where we operate as well as international norms. In 2013, Millicom became a founding member of the Telecommunications Industry Dialogue (TID), a group of telecom operators focused on privacy and FoE issues. TID has since merged with the Global Network Initiative (GNI), which includes more than 60 member organizations such as technology companies, ethical investors, academics and human rights organizations. GNI members work together in two mutually supporting ways. The GNI Principles and Implementation Guidelines provide an evolving framework for responsible company decision making in support of freedom of expression and privacy rights. As company participation expands, the GNI Principles are taking root as global standard for human rights in the ICT sector. GNI company members also participate in an independent assessment to determine their progress in implementing the GNI Principles. In 2019, Millicom underwent its first ever GNI Assessment process, marking the first time that telecommunications companies have been assessed as part of the GNI. Details on our assessment experience are included in this report.

An ever-evolving technological landscape creates greater challenges for government and law enforcement authorities across the globe. Increasingly, governments around the world are grappling with how best to regulate hate speech, remove extremist content and prevent misinformation campaigns while also preserving free speech. The phenomenon of "fake news" or disinformation campaigns via social media—which create tangible impacts on electoral events—is just one example of the challenges emanating from a data-centric society. Security agencies keep pushing governments to place greater public-safety obligations on technology firms. Conventional and established methods and procedures for requesting information related to criminal investigations are becoming outdated.

Prominent technology companies are advocating to extend or replicate provisions of the EU's General Data Protection Regulation (GDPR) in other jurisdictions to ensure uniform privacy protection. In Latin America, similar proposals have appeared across the region in the past few years. As technology evolves at an unprecedented pace, we are reaching a critical moment for ensuring respect for human rights both offline and online.

We must balance our respect for customers' human rights with our duty to comply with local laws in the countries where we operate. These laws require us to disclose information about our customers to law enforcement agencies and other government authorities in connection with their legitimate duty to protect national security and public safety, or to prevent or investigate crimes including acts of terrorism. Whenever we face a legal government request for customer information, we seek to minimize the impact of that request on our customers' right to privacy and FoE. Moreover, when any conflict arises between a local law and the Universal Declaration of Human Rights or other international human rights standards, we strive to resolve that conflict in a way that respects people's right to privacy and FoE, as well as their fundamental right to access the Internet and communications services.

Luxembourg, February 2020

Rachel Samrén
Executive Vice President, Chief External Affairs Officer

Salvador Escalón
Executive Vice President, General Counsel

2. Reporting at Millicom

Millicom is a leading provider of cable and mobile services dedicated to emerging markets. We operate under the Tigo brand in eight countries across Latin America and in Tanzania also. We also operate under the Cable Onda brand in Panama. Our company sets the pace in providing The Digital Lifestyle® to more than 50 million customers through our high-speed broadband and innovative services. Our purpose is to build the digital highways that connect people, improve lives and develop our communities. And our mission is to provide the fastest, most secure digital highways so that we become customers' first choice in all our markets. Millicom shares are listed on Nasdaq Stockholm in the form of Swedish Depository Receipts, and on the U.S. Nasdaq Stock Market since January 9, 2019.

We have published an annual LED report since 2015 for two key reasons:

1. To more transparently tell stakeholders how we deal with government requests, and
2. To more clearly explain the contexts in which telecommunications companies receive demands from governments and the considerations influencing decisions related to these situations.

As an operator focused solely on emerging markets, we strive to find the appropriate balance between providing high levels of transparency and protecting our staff and assets on the ground. In some markets where we operate, we are legally prohibited from disclosing law enforcement requests for assistance. In other instances, disclosure may place the safety of our staff and assets at risk. With this in mind, we subdivide our reporting into two regions—Central America and South America—to provide more granular and detailed information. Given our reduced presence in Africa, where we now only operate in Tanzania, this LED report only covers major events[1] in the Africa region overall, including major events related to our previous operations in Chad, which we sold to Maroc Telecom in July 2019.

We continually study and implement lessons learned from our industry peers and stakeholder engagement, predominantly through our association with the GNI and our interactions with government representatives. This report includes a section about our first-ever GNI Assessment completed in 2019.[2]

We hope this edition of our LED report will contribute to the constructive work among different stakeholder groups to better protect individuals' FoE and privacy.

What we report

We disclose the types and numbers of law enforcement requests we receive. More importantly, we also describe the overall context and trends reflected in the demands we receive. In specific and significant cases—what we call major events—the context serves to highlight practical challenges that we encounter in our interactions with law enforcement authorities.

We describe several of these major events and, whenever possible, disclose the countries in which they took place.

We disclose information about our internal policies, processes and controls that protect customers' privacy when we handle law enforcement requests. This report also describes how we seek to minimize unwarranted effects on our customers' freedom of expression and privacy.

Since the 2017 report, we have also included a specific country case study detailing the different types and sources of requests.

In addition, we include information about the various communications services we provide as well as the number of customers and our market position in each country. These details affect the number of requests we receive and should be considered when assessing the extent of government activities.

What we do not report

For the most part, this report describes our engagement in broad terms rather than detailing specific events. Law enforcement demands are sensitive in nature. In many cases, they relate to confidential court proceedings and to national security and emergency situations where human life is at risk.

Requests from law enforcement come with strict confidentiality requirements; often, we are prohibited by law from disclosing details about the requests we receive. Failure to comply with these requirements could lead to severe sanctions for our company and our local staff, including imprisonment.

Our ability to publicly discuss how we engage with law enforcement or other authorities when we receive requests, or the ways in which we challenge their approach, is limited. Doing so would affect our ability to engage with those authorities in the future and could, in some cases, put personnel at risk. Such limitations are a source of frustration at times, as they may lead to incorrect perceptions of inaction on our part.

Unlike some of our peers, we do not disclose the numbers of government requests by country. A major reason for not doing so is that certain countries prohibit such disclosure. Generally, the law is either unclear as to whether we can publish the numbers of requests received, or it explicitly prohibits publication.

We have conducted considerable internal risk analysis and debate about publishing country-specific numbers. We operate in some countries where publicly disclosing such numbers is likely to put the safety of our employees at risk. This is not necessarily a risk of action from the government; it could be from criminal entities whom the requests concern. In some countries, even beginning discussions with authorities

[1] Major events include politically motivated requests for (but not limited to): shutdown of our network, service denial or restriction, targeted take-down or blocking of content, denial of access for specific individuals with the intent to limit freedom of expression, significant operational changes relating to surveillance techniques, significant changes to local laws relating to government powers of surveillance or data retention, or requests to send politically motivated messages to customers on behalf of the government.

[2] Prior to our 2017 LED report, we reported our progress based on the TID principles. We now report against the GNI principles, following the completion of our first GNI Assessment process in 2019.

regarding disclosing numbers might, in our risk/benefit assessment, lead to negative outcomes for our operations and our ability to promote more rights-respecting practices.

For these reasons, we choose to aggregate numbers of requests at a regional level in this report. We split Latin America into Central and South America, which offers more granularity for the numbers.

We have worked with our former TID peers and with the law firm Hogan Lovells to create a legal frameworks resource https://globalnetworkinitiative.org/legalframeworks that details the government surveillance powers in our markets. For this reason, we do not outline specific laws by country in this report.

Definitions of requests

The information, communications and technology (ICT) industry has no agreed-upon definitions or classifications of law enforcement requests. Creating standard definitions is challenging given the multiple jurisdictions and business models in our wider sector. At Millicom, we classify law enforcement requests into three categories: interception, customer metadata, and customer financial data (related to the mobile money services or MFS services we provide). Some of our industry peers report in similar categories.

These three categories encompass the vast majority of requests we receive. We report all other requests outside of the definitions below as major events. We do not report specifically on content take-down requests, as they are relatively rare in our markets, with the exception of legally mandated removal of access to child sexual abuse content in Colombia. However, we have seen increasing requests for take-down of online content in recent years, although this content often is not under our control and can only be taken down by the host content provider. We are also seeing various legislative proposals to mandate the removal of illegal content online. When applicable, we account for content takedown requests in the Major Events section of this report.

How we obtain the material we report

We receive information on the number of law enforcement demands from the legal and regulatory departments in each of our local operations. As prescribed by our **Law Enforcement Assistance and Major Events Guidelines**, these departments receive all demands and review their legality before executing the demands. Our departments log each demand by date, type (see Table 1) and requesting authority. Once a request is legally justified, we provide the information to authorities or undertake the necessary actions.

Information about interception, metadata and mobile money-related requests is collected during our annual corporate responsibility reporting process through Enablon, a dedicated tool into which local legal teams enter total amounts of requests as well as evidence for their aggregated numbers.

We report information related to major events according to an escalation mechanism defined in our **Law Enforcement Assistance and Major Events Guidelines.**

The Global External Affairs team maintains a log of information about all major events, which are reviewed in our cross-functional LED Committee comprised of senior staff from the External Affairs, Legal, Security and Compliance functions. ERM Certification and Verification Services (ERM CVS) has assessed Millicom's numerical information related to law enforcement demands as part of our corporate responsibility reporting limited assurance process, as disclosed in our Annual Report on pages 57.

Feedback

We are keen to hear from, or work with, anyone seeking to promote open access and transparent and accountable processes for surveillance and security. We also welcome feedback on this report or on privacy and FoE issues in general. Please contact CR@millicom.com or find our full contact details at www.millicom.com.

Table 1
Request categories

Interception	Interception of voice, SMS, fax and data traffic (lawful interception) in real time; i.e., live surveillance.
Customer metadata	Metadata such as call data records, IP addresses, SMS, email traffic, Internet traffic information, documents from Cloud services, and requests for location information (physical/base station or GPS).
Mobile money services-related data	Information related to our mobile financial services (MFS), such as transaction data, confirmation that an individual is a mobile money customer, and other account activity. These requests do not always relate to a financial crime.

3. Our governance and engagement

We have long recognized the need to engage civil society, NGOs, investors, customers, academia and subject-matter experts on privacy and FoE to enhance our understanding of human-rights risks related to our operations, and enact processes to manage those risks.

Our actions to minimize risks where possible include introducing and updating Millicom guidelines, adding controls, and improving the readiness of local and global teams to handle any major events as well as the human rights and reputational issues that such events pose. We initially focused on improving local processes by providing support to local management and the teams that manage law enforcement relationships. Since then, we have progressed significantly—instilling a culture of respect for privacy and FoE rights throughout our business and acting as a thought leader in emerging markets on these topics.

In 2018, we began our first external GNI Assessment process (discussed in more detail in chapter 4). We have also reviewed and strengthened our existing policy framework created in 2015. This largely involved streamlining and consolidating our previous work, as well as making updates in line with technological advancements and the evolving political and security environments in our operations. Our **Global Privacy Policy**, addresses customers' privacy rights.

Human rights impact and risk

In 2017, the first year of our GNI membership, we carried out a global human rights risk assessment of our operating environment to assess the risk level for major events or other requests that may pose threats to our customers' rights. We derived the salient and material risks posed by each country from VeriskMaplecroft's risk indices.[3]

As part of this risk assessment, we engaged external expert support to evaluate all our policies, practices and resources so that we could better understand our potential risks and the opportunities to improve.

Our significant on-the-ground presence in our markets gives us a strong understanding of potential risk situations and risk levels. We sought to formalize this assessment and broaden our analysis by interacting with internal and external stakeholder groups to create a dynamic tool that we could update and consult regularly. In 2018, we worked with leading sustainability firm Business for Social Responsibility (BSR) to build a Human Rights Impact Assessment (HRIA) toolkit, which we deployed in select local operations in 2019. We will continue to roll out this assessment across our operations in 2020.

BSR also supported us in our most recent Materiality Assessment, convening internal and external stakeholder interviews to help define Millicom's priorities in the corporate responsibility space. Naturally, privacy and FoE were key areas of focus during this assessment.

Governance and oversight of human rights

Corporate responsibility is a core function within our External Affairs team. Millicom's Board of Directors (BoD) and our Executive Team (ET), which includes the EVP Chief External Affairs Officer, oversee our corporate responsibility activities. The Board receives regular updates on corporate responsibility topics with Millicom's CEO, EVP Chief External Affairs Officer, and EVP General Counsel attending the BoD meetings. The EVP Chief External Affairs Officer also reports to the ET on these topics on a monthly basis, while Millicom's Corporate Responsibility Director is responsible for ongoing management of human rights issues in the company.

Our BoD receives periodic updates on human rights issues and has directed management to continue its strong proactive approach, which includes deepening relationships with civil society at the country and global level. During 2019, the BoD received updates on Millicom's implementation of the GNI Principles and our management of risks related to privacy and FoE from the EVP Chief External Affairs Officer. The BoD's Compliance and Business Conduct Committee also provided additional oversight.

In January 2014, when Millicom began its escalation process for government requests, we established a cross-functional Law Enforcement Disclosure (LED) Committee to better coordinate risk management. This committee is chaired by the EVP Chief External Affairs Officer and includes the Director of Corporate Responsibility, EVP General Counsel, EVP Chief Ethics and Compliance Officer, Chief Information Security Officer, VP Legal Latam and Global Chief Privacy Officer, VP of Compliance Strategic Response and our Regulatory Affairs Directors. LED Committee members prepare and jointly approve policies and processes, review our **Law Enforcement Assistance and Major Events Guidelines** and related risks, and approve Millicom's reporting and engagement related to privacy and FoE. The LED Committee communicates frequently and met on several occasions in 2019 to review risks and actions related to FoE and privacy, and to receive updates on Millicom's ongoing GNI Assessment process. These meetings provided an opportunity to brief and introduce new team members on our ongoing work on these issues, while helping to assess and define 'Major Events' in our markets. This Committee also provides guidance and input on how Millicom can best approach these issues in both a rights-respecting and law-abiding manner.

[3] https://maplecroft.com

We completed our **Global Privacy Policy** framework in 2018 and continued to execute it through 2019. In addition we have approved broad privacy principles, guidelines and commitments for the company. At a global level, our Privacy Office is led by our Global Chief Privacy Officer. At a local level, all Tigo operations have a Local Privacy Officer responsible for the administration of privacy matters and local training. Our Millicom and Tigo websites provide information to our customers regarding our **Global Privacy Policy**, including how we use, process and protect customer data, their rights related to the use of their data, and channels and contact points where our customers can raise concerns about our policy or their privacy.

Our EVP Chief External Affairs Officer, EVP Chief Ethics and Compliance Officer, EVP Chief Technology and Information Officer, Global Chief Privacy Officer and EVP General Counsel monitor the privacy framework development efforts. We continue to roll out this framework internally and externally along with Millicom's privacy commitments and guiding principles. All relevant information is available in our online privacy policy portal at http://www.millicom.com/privacy-policy/.

Engagement

We work with a wide range of actors to mitigate human-rights impacts and risks related to law enforcement requests. Millicom is a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy; in 2017, we joined the Global Network Initiative (GNI) as a full member. We also engage with many international organizations, taking part in various events and contributing to the ongoing debate around FoE and privacy in the context of a rapidly changing technological landscape. We developed and expanded our relationships with civil society actors through our membership in the GNI during 2019, participating in the GNI's Policy Committee and Learning Committee to further mutual interests in the defense of FoE and privacy rights. In addition, we engage as much as possible with governments and other in-country stakeholders on FoE and privacy topics. We seek to enhance governments' understanding of our obligations outside of their countries while also highlighting the risks from disproportionate government action, especially to governments' reputation and foreign investment possibilities. We also discuss these topics with relevant diplomatic representatives. We conduct similar conversations and trainings with our local staff members who engage with these issues on the ground.

A rapidly changing technological environment and high public-security demands can complicate our decision-making process as we strive to adhere to legal obligations and protect the FoE and privacy of users. We provide yearly face-to-face training on these topics with our local staff at regional summits, as well as specific training sessions with, and in, different operations as needed.

Policies, guidelines and controls

We include a commitment to the International Bill of Human Rights and the UN Guiding Principles on Business and Human Rights in the **Millicom Code of Conduct.**

In addition, our commitment to implement the TID's Principles on Freedom of Expression and Privacy for the Telecommunications Sector was based on our TID membership. Millicom's LED reports began as a public accounting of our commitment. We now adhere to the GNI Principles on FoE and Privacy, and report more extensively on these commitments following our first GNI Assessment process.

During 2018, the LED Committee finalized and approved updates to **Millicom's Group Guidelines for Law Enforcement Assistance (LEA) and Major Events**, which comprise a streamlined, consolidated version of our various internal policies and work in this area. These guidelines summarize:

- Our obligations within international frameworks
- Roles and responsibilities of each department
- Assessments to be conducted as requests are received
- How to handle urgent and non-written requests
- How to log requests and our responses
- How to protect customer data throughout the process of retrieving information
- How to deliver the information safely

A shortened version of this guideline is available at www.millicom.com/media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf.

We also adopted a new **Governance Process for Human Rights Risks Related to Freedom of Expression and Privacy**, which allocates responsibility for the company's implementation of the GNI Principles among several members of Millicom's senior management team. The EVP Chief External Affairs Officer and EVP General Counsel, working with senior members of the Corporate Responsibility, Legal and Compliance teams, are ultimately responsible for the company's implementation of the GNI Principles related to privacy and FoE rights.

Our **internal control process** assesses how well our local operations apply, and comply with, various global policies and controls. In 2015, we added two controls related to the implementation of the original LEA Guidelines. The first control verifies that all requests are assessed by the legal team before execution and that a written copy of the original request is retained on file. The second control relates to limiting and making a log of access to customer data when executing the request. Our operations assess their alignment—or maturity level—with these controls annually. All operations have made substantial improvements in the maturity level of their controls for the LEA guidelines since 2015. In 2019, we began revising our internal control processes in line with changes made to our policies concerning FoE and privacy; we will continue this analysis during 2020.

The LED Committee approved **Major Events Guidelines** in 2015. These guidelines define steps to take in the case of a major event, including a regional and global escalation process, as well as

practical suggestions for engaging with government authorities to limit the remit and/or timeframe of a major event. In 2017, we began assessing how to streamline communication of these internal policies, guidelines and controls to our local staff. We conducted an external benchmarking of how this is done across the industry before deciding to create one authoritative document called the **Law Enforcement Assistance and Major Events Guidelines**.

We did this to ensure our internal resources are easily understood and so that they remain relevant in an ever-evolving environment. We train staff members on these topics regularly.

Information security

The Millicom **Information Security Standards** (ISS), published in April 2015, address specific requirements for managing customer and employee data.

All Millicom employees must take Information Security training, which addresses the importance of protecting customer data. The training material is available at our eLearning platform, Millicom University, and is mandatory for all employees. We also distribute IS awareness materials to all employees at least annually.

4. GNI Assessment

During 2018–19, Millicom and 10 other member companies underwent the GNI Assessment process. This marked the first time that telecommunications companies have been assessed as part of the GNI.

Millicom's accredited external assessor Foley Hoag[4] presented its findings and recommendations to the multi-stakeholder GNI Board of Directors, which determined that Millicom is making good-faith efforts to implement the GNI Principles with improvement over time. The Board's positive determination was based on a report from the expert external assurer which assessed Millicom's processes, policies and governance model to safeguard users' FoE and privacy.

The GNI Assessment involves a Process Review covering: governance, due diligence and risk management, FoE and privacy in practice, and transparency and engagement. The process also includes a case study review that analyzes specific examples or situations to verify whether the company is implementing FoE and privacy principles in practice.

The following sections provide a brief overview of Millicom's GNI Assessment results, aligned with the above-mentioned areas.

Governance

Ultimate responsibility for Millicom's implementation of the GNI Principles rests with the company's General Counsel and its Chief External Affairs Officer. Operational responsibility for the development, implementation, and execution of policies and procedures rests with the company's Legal team for the right to privacy, and with the Corporate Responsibility function within the External Affairs team for the right to FoE. Millicom's BoD receives updates on the company's implementation of the GNI Principles and its management of risks relating to the privacy and FoE rights of its users at its quarterly meetings.

Due diligence and risk management

Millicom incorporates human-rights due diligence into its routine corporate due diligence and enterprise risk management processes. Our Law Enforcement Assistance and Major Events Guidelines empower, and obligate, frontline personnel to escalate potential issues for due diligence. According to the policy, changes in a country's operating environment that materially increase the risks posed by Millicom's operations to the FoE and privacy rights of its users are major events that must be reported immediately to senior staff members.

We prioritize the human-rights risks identified by our due diligence processes based on the severity of the likely impacts, our ability to mitigate those impacts, the safety of our employees, and the integrity and reliability of our operations. In 2017, we engaged an external consultant to conduct a HRIA of Millicom's global operations. This exercise identified Millicom's most salient risks and laid out measures that the company could take across its operations to mitigate its potential and actual adverse human-rights impacts. Furthermore, the HRIA evaluated the legal and regulatory environment in each of the 11 countries in which Millicom operated at the time and identified future risk scenarios in those countries in the coming years.

The results of Millicom's HRIAs are incorporated into our operations and business processes primarily through the work of our in-house Corporate Responsibility team. The most important way that we mitigate the human-rights risks identified through our due diligence processes is by creating robust systems to help frontline personnel respond to government requests and demands.

FoE and privacy in practice

Millicom's Law Enforcement Assistance and Major Events Guidelines direct our assessment of and response to government restrictions and demands that impact the privacy and FoE rights of our users. We distinguish between two categories of requests:

1) Government requests for user data that are issued in writing and appear be consistent with local law and international human rights standards. We log these requests in a database maintained by Millicom's in-country, in-house legal team and which our corporate team audits yearly. Our in-country lawyers study each request to verify that it complies with local legal requirements. If so, Millicom grants the request on the narrowest possible basis. If not, Millicom rejects the request and explains its reasons to the requesting government entity.

2) Government requests and demands that are not made in writing, are obviously inconsistent with local law or international human rights norms, conflict with the terms of Millicom's operating license in that country, and/or appear to be politically motivated. These are considered major events that must be escalated to the company's executive-level personnel for review and decision. Once a major event is escalated, Millicom's senior personnel evaluate the range of available options before formulating a response. We attempt to balance our responsibility to respect international human-rights norms with our obligation to follow local laws in the countries where we operate.

[4] https://foleyhoag.com/

Transparency

Privacy and FoE are Millicom's most important corporate responsibility topics, according to our most recent Materiality Assessment and our annual LED Report details our policies and procedures to protect the rights of the company's users in the face of specific government demands.

We provide an independent ethics hotline for employees, customers, investors and the public to report violations of the law or company policies, or to raise concerns about other forms of alleged misconduct. Callers may characterize their concerns as being related to "Data Privacy and Protection" or "Compliance with Laws and Regulations."

Case study review

The GNI Board reviewed a number of case studies, including cases related to specific government requests and demands concerning FoE and privacy. The board also reviewed other categories of suggested cases from the Assessment Toolkit.

Some of the cases included previously reported major events and/or reviews of how our relevant policies and guidelines work in practice. The GNI Public Assessment Report[5] provides details on selected cases such as prison "signal blocking" laws in Latin America and the Digital Fingerprint Bill in Paraguay.

[5] https://globalnetworkinitiative.org/wp-content/uploads/2020/04/2018-2019-PAR.pdf

5. South America

Overview

Millicom has operated communications networks in South America for more than 25 years. We provide a wide spectrum of services—including high-speed data, cable TV, voice and SMS, Mobile Financial Services (MFS), and business solutions—in three South American countries. During 2019, we invested a combined total of over US$1 billion in the South America and Central America regions to further develop our mobile and fixed communications networks. These investments ensure better bandwidths and quality of Internet experience. They also allow more services and innovation to be built on top of the access that we provide.

We hold the top market position in business-to-consumer (B2C) mobile, B2C home and MFS in Paraguay and are generally ranked among the top three providers across those services in Colombia and Bolivia. We are an important contributor to our markets in terms of investment, taxes paid,[6] and the employment and services we provide. For more details, see the tables below and our socio-economic report at https://globalnetworkinitiative.org/policy-issues/legal-frameworks/.

Table 2
South America (Bolivia, Colombia and Paraguay)

	B2C Mobile Customer Relationships[7] '000	MFS customers '000
	15,838	2,657	1,553

Table 3

Country	Mobile Customers '000	Workforce[8]	Population[9] '000
Bolivia	3,554	2,877	11,353
Colombia	9,114	4,325	49,648
Paraguay	3,170	5,511	6,956

Legal frameworks

In Bolivia and Paraguay, clear processes and requirements exist for judicial oversight over interception and customer metadata requests. In Colombia, due largely to the long-lasting internal conflicts and war on drugs, the processes are significantly more complex—although judicial oversight does exist for initiation of interception. Information about the laws and procedures in Colombia is published in detail at https://globalnetworkinitiative.org/policy-issues/legal-frameworks/.

In Bolivia, the use of interception is restricted to exceptional circumstances, such as human and drug trafficking, in which we would receive court orders to activate lines. We have ongoing discussions with authorities regarding the implementation of interception techniques. Concern about the security environment in Bolivia following the recent election crisis may fuel debate over further monitoring and control mechanisms for communications services.

Procedures in Colombia require us to provide direct access for authorities to our mobile network. Regular audits ensure we do not obtain information about interception taking place. We are subject to strong sanctions, including fines, if authorities find that we have gained such information. As a result, we do not possess information regarding how often and for what periods of time communications are intercepted in our mobile networks in Colombia. We also have a significant fixed-network business in Colombia; for these lines, we receive judicial orders which we review and assess before opening the line for interception to take place. Length of interception is limited in the law to a maximum of six months.

In Paraguay, as in Colombia, authorities mandate that we provide direct access to our mobile network. The procedures allow us to view the judicial order required for authorities to initiate the interception, and we are aware when interception occurs. We can file a complaint before the Supreme Court of Justice should we deem that the order or interception does not follow legal requirements.

For customer metadata requests, we receive written orders in all three countries. We assess these requests for their legality before providing authorities with the requested information.

[6] See page 159 in our Annual Report.
[7] Total number of households with an active service.
[8] Workforce accounts for employees directly employed by Millicom.
[9] Population statistics as per World Bank (2018).

Law enforcement requests in 2019

Table 5 shows an increase in the requests received from law enforcement authorities across our markets in South America. However, the numbers have stayed relatively consistent since 2015. A notable increase in the number of interception (i.e., live or real-time call surveillance) requests has resulted from the full implementation of a direct access system in one country after technical changes. We have also seen a gradual increase in MFS-related requests as this business grows and becomes more popular in our markets.

A number of countries in the region have direct access to our networks. Depending on the type of direct access concerned, this can often mean we are not notified of all instances in which customer communication is being intercepted. The actual written request received by an operation counts as one request in the data tables. A request may seek information about several individuals or several devices. Therefore, requests are not equal in magnitude.

The vast majority of requests are in the category of customer metadata. Most of these requests, in turn, seek to confirm the identity behind specific phone numbers. Some requests may ask for information about more than one customer's mobile phone records (e.g., calls to and from the phone, cell tower location, during a specified time period or within a specific geographic area).

The number of requests that our local operations receive also depends on how many customers we have and our market position. In South America, the percentage of metadata requests received per customer in 2019 was 0.157%, nearly identical to the 2018 figure.

Table 4

	Authorities that can request interception or metadata	Authorities that can issue orders for interception
Bolivia	Prosecuting attorneys, Unit of Financial Investigations	Judicial authorities
Colombia	The military, the police, Prosecutor General, Civil Servants with judicial or oversight functions, Comptroller General, Attorney General, Mayors, and the National Penitentiary and Prison Institute (INPEC)	Attorney-General's office and judges
Paraguay	Public Prosecutor's Office, Criminal Courts	Criminal Courts

Table 5

South America	Interception	MFS	Metadata	Metadata requests per customer
2019	732	239	24,864	0.157%
2018	583	190	22,590	0.154%
2017	38	21	21,492	0.150%
2016	111	73	22,521	0.103%
2015	184	104	24,447	0.115%

6. Central America

Overview

Millicom has operated in the Central America region for more than 25 years. We provide a wide spectrum of services in six different markets including high-speed data, cable TV, voice and SMS, Mobile Financial Services (MFS), and business solutions. During 2019, Millicom invested a combined total of over US$1 billion in the South America and Central America regions to further develop our mobile and fixed communications networks. These investments ensure better bandwidths and quality of Internet experience. They also allow more services and innovation to be built on top of the access that we provide.

We hold the top market position for many services across the region. Also, we are an important contributor to our markets in terms of investment, taxes paid,[10] and the employment and services we provide.

In addition to the five countries we are reporting on in 2019 (Costa Rica, El Salvador, Guatemala, Honduras and Panama), we recently acquired new assets in Nicaragua. We had previously only catered to enterprise clients, and a very small number of cable TV and DTH customers in Nicaragua until mid-2019, when we closed a transaction for the takeover of Telefonica's mobile business in the country. While we have previously reported on major events linked to Nicaragua, moving forward we plan to include numbers for all parts of the newly acquired businesses in this particular section also.

We also completed the takeover of Telefonica's business in Panama in September 2019. The numbers related to Panama in this section of the report only pertain to the Cable Onda business, of which we became 80% shareholders in December 2018.[11] We also plan to include numbers for all parts of the newly acquired businesses in Panama in this particular section going forward.

From the beginning of our involvement in these new operations, we have trained staff members on our key policies and guidelines in the areas of FoE and privacy.

Legal frameworks

Due to challenging security environments—including high levels of organized crime and drug trafficking–related violence—governments in Central America have enacted some of the most-developed laws and technical surveillance requirements. In Costa Rica, where we currently operate fixed networks only, the number of law enforcement requests is significantly lower than in other Central American markets. This is also true about the numbers for Panama in this year's report, as we are only including requests related to the Cable Onda business. We plan to report on the newly acquired Telefonica assets in Panama, Nicaragua and Costa Rica—of which the latter is still subject to regulatory approval—starting in 2020.

Table 6
Central America (Costa Rica, El Salvador, Guatemala, Honduras and Panama)

B2C Mobile customers '000	Customer Relationships[12] '000	MFS customers '000
22,488	1,683	1,997

Table 7

Country	Mobile Customers '000	Workforce[13]	Population[14] '000
Costa Rica	N/A[15]	513	4,999
El Salvador	2,465	639	6,420
Guatemala	10,536	3,342	17,247
Honduras	4,473	1,028	9,587
Panama	N/A[16]	2,218	4,099

[10] See page 159 in our Annual Report.
[11] In February 2019, Millicom entered into agreements with Telefónica S.A. and certain affiliates to acquire the entire share capital of Telefónica Móviles Panamá, S.A., Telefónica de Costa Rica TC, S.A., wholly owned subsidiary Telefónica Gestión de Infraestructura y Sistemas de Costa Rica, S.A., and Telefonica Celular de Nicaragua, S.A. for a combined enterprise value of US$1,650 million. This transaction is subject to regulatory approvals in each market – these approvals have been secured in Nicaragua and Panama, while Costa Rica is still pending.
[12] Total number of households with an active service.
[13] Workforce accounts for employees directly employed by Millicom.
[14] Population statistics as per World Bank (2018).
[15] Millicom does not presently have mobile operations in Costa Rica but does have B2C home and B2B services, in which it is the market leader.
[16] The numbers related to Panama in this section of the report only pertain to the Cable Onda business, which does not have mobile operations.

In Honduras and El Salvador, the law mandates direct access to our networks by the authorities. However, the laws in both countries specify which authorities can request interception, and the actual interception orders can only be granted by the courts (see Table 8). As these are direct-access regimes, we do not receive these orders nor do we have visibility into how often or for what periods of time interception takes place. In El Salvador, the law also lists the types of specific crimes to which interception can be applied in addition to other requirements. In Guatemala, interception also takes place under judicial orders, which we receive and review before opening the line for the specified time period.

For customer metadata, judicial orders from the same courts are required in all of our markets in Central America. We receive and review these requests before we provide the authorities with the requested information.

In El Salvador and Honduras, special laws require telecommunications operators to block signals in and out of prisons. Similar laws had previously existed in Guatemala, while Costa Rica recently introduced legislation in this area. See section 9 for a more extensive overview of prison signal blocking in the region.

We are not compensated for the resources required to assess and process requests from law enforcement in any of our markets. Given the challenging security situation in numerous Central American countries, these resources are extensive and must be available to respond to requests at all times.

Law enforcement requests in 2019

Law enforcement authorities across our markets in Central America continue their efforts to tackle crime and violence in the region. These countries rank among the most violent in the world, with annual homicide rates in El Salvador and Honduras that meet or exceed the most lethal periods of recent wars in Afghanistan and Iraq. Notorious transnational criminal gangs involved in activities ranging from drug smuggling to human trafficking are largely responsible for the violence afflicting these countries. Surveillance and customer data requests underpin law enforcement authorities' efforts to combat these serious challenges of organized crime. Differences in the populations of our Central American and South American markets add to making direct comparisons from one region to the other difficult. Also, as mentioned previously, law enforcement requests are not all equal in magnitude, which further complicates any attempt to make direct comparisons.

As shown in Table 9, request types have remained at relatively similar levels to those seen in 2018. Certain requests may involve a large number of metadata records, which can skew the numbers. Efforts to combat crime and corruption in one particular country continue to drive a large proportion of these requests, and such efforts remain the primary reason behind certain requests. Also, as the innovative MFS business segment grows more popular, it is drawing increased attention from authorities.

Table 8

	Authorities that can request interception or metadata	Authorities that can issue orders for interception
Costa Rica	Prosecutor's Office, Judges and Tax Authority	Judges in Criminal Courts
El Salvador	Attorney General's Office	First Instance Court of San Salvador
Guatemala	Prosecutor's Office	Judges of First Instance in Criminal Matters
Honduras	Prosecutor's Office, Attorney General, National Investigation and Intelligence Office	Criminal Court
Panama	Attorney General's Office	Judicial branch

Table 9

Central America	Interception	MFS	Metadata	Metadata requests per customer
2019	1389	275	12,633	0.072%
2018	1533	333	11,278	0.064%
2017	933	160	10,848	0.060%
2016	816	194	16,758	0.099%
2015	0	158	8,653	0.052%

7. Case study

In 2017, we decided to provide more specific details about the types and sources of requests received in one unnamed country. Since then, we have continued providing the same details for the same country to create a year-to-year data comparison.

We chose to anonymize this data to respect local disclosure requirements and protect our local staff. We hope this level of detail will provide further context to the nature of government requests and demonstrate the complexity and variety of factors involved in these processes.

Types of requests related to metadata

The following information is a snapshot of what type of metadata requests were received in one of our local operations.

Sources of requests related to metadata

Requests come from a range of sources. The Attorney General's Office, the National Police and the country's judiciary continue to generate most requests. These requests arrive with prior authorization from a relevant court or judge and are assessed for validity by our local legal team, which authorizes or refuses the request accordingly.

Table 14
Customer metadata requests

Type	Percentage of Total (Jan–Sept 2017)	Percentage of Total (Jan–Sept 2018)	**Percentage of Total (Jan–Sept 2019)**
Biographical details (owner of phone number)	58.05%	54.87%	**47.26%**
Call and event registers	34.79%	38.16%	**44.67%**
Details related to potential acts of fraud	3.05%	3.28%	**3.10%**
Contract copies or originals	3.08%	2.61%	**2.75%**
Coverage data and antenna locations	3.20%	0.04%	**1.40%**
IP Address location	0.12%	0.96%	**0.62%**
PUK Code (to unlock SIM card)	0.02%	0.06%	**0.01%**
Requests to redirect emergency service calls	0.07%	0.02%	**0.00%**

Requestor	Percentage of Total (Jan–Sept 2017)	Percentage of Total (Jan–Sept 2018)	**Percentage of Total (Jan–Sept 2019)**
Attorney General's Office	46.86%	47.93%	**46.04%**
National Police	33.91%	34.55%	**33.66%**
Other Entities	7.67%	7.45%	**9.58%**
Judges	10.76%	9.55%	**8.53%**
National Army	0.49%	0.20%	**1.45%**
Lawyers*	0.03%	0.14%	**0.43%**
General Comptroller of Accounts	0.15%	0.05%	**0.11%**
National Tax Authority	0.12%	0.08%	**0.11%**
Private Entities*	0.00%	0.03%	**0.05%**
Department of Security	0.00%	0.01%	**0.00%**

* These numbers refer to requests that were previously authorized by a court or judge.

8. Major events in 2019

Major events are requests that fall outside of the three types of law enforcement assistance covered in previous sections of this report. All local operations are required to escalate these events to global management and take steps to minimize the effect of such events on our services and on our customers' rights to FoE and privacy. The events described in this section were reported to global headquarters in 2019.

Deciding whether to challenge a major event is rarely simple. These requests often have a legal basis, although the events frequently stem from broad national-security—related powers.

Major events include:

- Requests for shutdown of specific base station sites, geographical areas or an entire network
- Service denial or restriction (SMS, mobile/fixed Internet, social media channels)
- Interception requests outside of due process
- Targeted take-down or blocking of specific content[17]
- Denial of access for specific individuals
- Significant changes related to surveillance techniques or operational processes (how local surveillance laws are implemented in practice)
- Significant changes to local laws related to government powers of surveillance or data retention
- Requests to send politically motivated messages to customers on behalf of the government

In 2019, we recorded ten major events, a significant decrease compared with 2018 and previous years, as shown in Table 16. Eight of the events occurred in Africa and two occurred in Central America.

Year-to-year comparisons of our major events are difficult, given that we have divested from a number of operations in Africa while refocusing our capital and efforts on existing and new markets in Latin America. Given the significant proportion of major events in the Africa region, however, we have chosen to include those events in this section.

As with law enforcement requests, the ICT sector has no accepted or standardized definitions for different types of major events or how to account for them.

Millicom counts the number of requests made directly to us as well as events that have consequences or implications to our services and the rights of our customers.

We count the event regardless of whether or not our engagement was successful in preventing it. One request may include a shutdown of several different services or parts of the network in several different geographical areas. If we receive a request to extend a previous shutdown, we count this as a new event.

For example, in the case of a request to shut down cell towers around prisons in Central America, we count one request per country instead of the number of prisons or cell towers involved. In the case of prison shutdowns which are ongoing with no significant changes in terms of obligations or requirements, we do not count this as an additional event; for 2019, we recorded no major events in this area. Although we do not report ongoing signal blocking in prisons (or new blocking measures which do not impact our business directly) as a major event, we consider this a significant issue and continue to provide details on its implications and the work we are doing to mitigate risks and threats to FoE.

We have clear guidelines for our subsidiaries on handling major events in addition to escalating the information to the global team for assistance. For some of the events below, we are unable to describe how we reduce the impact of these events on our customers' privacy or FoE. However, we have shared such information in different multi-stakeholder forums such as the GNI.

Table 16
Type of major event

	2015	2016	2017	2018	2019
Shutdown or restriction of services	8	8	2	7	8
Proposal for significant changes in local laws	3	5	4	5	1
Proposal for significant changes in technical or operational procedures	3	2	1	2	1
Disproportionate customer data or interception requests	2	1	2	2	0
Politically motivated messages	2	1	0	1	0
Other	2	1	5	3	0
TOTAL	**20**	**18**	**14**	**20**	**10**

[17] With the exception of blocking child sexual abuse content.

Shutdowns or restriction of services

When we receive requests for shutdowns or service restrictions, we must consider direct consequences for our local operation and management if sanctions defined by law are applied. Sanctions may include fines, imprisonment or removal of a license to operate communications networks. Requests for shutdowns or service restrictions often happen during a particularly volatile time, which means we must also consider the safety of our staff as well as potential retaliation from the general public against our company and our visible assets, such as shops and base station sites.

Chad

In 2019, government-mandated disruptions to Internet and social media access continued across the Africa region. In Millicom's markets, a 16-month social media block in Chad ended in July 2019. We included this major event in our 2018 LED report but not in this year's numbers. As per previous years, we received numerous base station shutdown requests in Chad during 2019 as the country's security forces continued to fight terrorist threats. Millicom sold its operations in Chad to Maroc Telecom in June 2019, so this year's report includes country-specific information on Major Events only up to that point.

Tanzania

Although we have not received any shutdown orders in Tanzania, we continue to receive specific content takedown requests for betting websites. Although we do not deem these requests to be politically motivated or nefarious, we remain consistent in our reporting of the requests as major events. We carefully review and discuss takedown requests that are not related to child sexual abuse content.

We consistently flag such events and send them through our robust escalation process. This demonstrates how seriously our staff adheres to Millicom's internal guidelines.

Informing customers of shutdowns

In our markets, mobile services are primarily pre-paid and our customers interact with a large distribution base that consists of individual entrepreneurs and small convenience stores. We meet with our sales force daily to inform them of new promotions, products or other relevant issues. This enables us to carry messages to customers through our sales force, even when our services are affected.

In the event of government-mandated service disruption, we do our best to notify customers that we are dealing with a situation beyond our control. In most cases, our customers know why services are not available.

Ongoing shutdown of services in prisons in Central America

Since 2014, authorities in El Salvador and Honduras have enacted laws that oblige all telecommunications operators to shut down services or reduce signal capacity in and around prisons, where the authorities suspect criminal gangs continue to operate by using smuggled cell phones. Guatemala enacted similar laws in 2014, but the relevant legislation was overturned in the Supreme Court in 2015. Costa Rica also introduced new signal blocking measures in 2018. We assisted with monitoring and advocacy work performed by organizations such as the GSMA and ASIET and will continue to work with the Costa Rican government on this issue after we close the acquisition of Telefonica's mobile assets in the country.

In Central America, where prisons are often located in urban areas, actions such as removing antennas, shutting down base station towers and installing signal jammers can affect mobile service for people living near the correctional facilities. For example, ATM use may be disrupted. Sanctions for non-compliance with these lawful orders include substantial fines and the possible revocation of licenses.

We continue to engage with local authorities and industry peers on finding alternative ways to address signal blocking in and around prisons that do not affect nearby residents. These alternatives include new network coverage designs around prisons, third-party solutions that block signals in specific physical areas, and relocation of prisons to less densely populated areas.

Millicom underwent an external assessment of our case study on prison signal blocking in the Central America region as part of the GNI Assessment process. The GNI Public Assessment Report includes a description of this case study.

El Salvador

El Salvador approved an Anti-Extortion Law in April 2015 that prohibits any telecommunications signal inside a prison. This legislation established daily fines of up to US$900,000 for non-compliance and authorizes the government to revoke the license of any telecommunications operator that receives five fines within a year.

As violence in the country peaked in early 2016, the National Congress approved a law that allowed the government to take specific and drastic actions related to at least seven prisons if telecommunications operators did not block their signals in the vicinity. In 2018, the Legislative Assembly's Security Commission reformed the "Penitentiary Law" to make signal blocking a permanent rather than temporary mechanism. Because of this legislation, Millicom and other operators had to shut down base station towers not only near the prisons but also in surrounding areas, leaving part of the population without service. Our company has since narrowed the scope of our blocking measures to help mitigate FoE impacts for nearby customers.

Immediately after the government enforced these extraordinary measures, we informed our customers about the shutdowns and their possible implications on our services, explaining that we are obligated to comply with the measures related to national security efforts. Telecommunications operators in El Salvador continue to work with the new government authorities, which changed in June 2019 when President Bukele took office, to reduce and minimize the service impacts. A joint working group has been established with the authorities in order to monitor progress and the functioning of jammers in prisons. Operators will also donate additional equipment to monitor and locate devices within certain prisons.

Honduras

On January 2014, the National Congress of Honduras passed a law requiring operators to block any telecommunications signal from reaching the country's prisons.

The sanction for non-compliance is approximately US$420,000 for the first instance and approximately US$840,000 for the second, while a third violation can result in license termination. In 2014, operators turned off several antennas to comply with the law, leaving some users in large cities without service. Operators have yet to find a blocking solution that limits the effects on people outside a prison but also does not allow prison guards to turn off the jammers.

In 2016, we had to extend signal blocking to three additional prisons and improve the effectiveness of previously installed jammers. CONATEL, the Honduran telecommunications regulator, sent written notification about a sanctioning process after running tests at one of the prisons where CONATEL had detected a signal that permitted outgoing calls. In January 2017, both Tigo and the country's other large operator, Claro, were served with sanctions for outgoing calls. We are still disputing this sanction in the courts. The situation remained much the same throughout 2018 and 2019.

Proposals for significant changes in operational procedures or local laws

Local laws strictly prohibit Millicom from disclosing details of proposed changes in law enforcement procedures, such as changes to operational procedures of law enforcement assistance. These procedures define how local laws regarding such assistance are implemented in practice and detail how day-to-day requests from law enforcement are made and handled.

Regulators and legislators continue to scrutinize local legal frameworks and operational procedures in many of our operating markets. Building off a similar trend in Central America, the major events that we recorded in Latin America during 2019 involved a proposed new cybercrime bill and operational changes to procedures for telephone call interventions, both in Costa Rica.

We engage with local authorities to develop laws through an open and consultative process. Our most frequent request to legislators is that they establish judicial oversight; promote proportionate and necessary measures; and be as narrow, clear and detailed as possible regarding which authorities can make requests under the law and how the law requires us to respond. We often find that legislators struggle to understand the roles and limitations of different players in the ICT ecosystem. As a result, legislators often assign requirements to telecommunications companies that can only be carried out by providers of specific services.

We also do not agree that telecommunications operators should bear the cost of implementing technical and operational measures for interception, as is frequently proposed by governments. In our view, sharing these costs will help encourage the proportionate use of such powers.

Costa Rica

Draft bill No. 21187, which seeks to combat cybercrime, includes language calling for the preservation and safeguarding of subscriber information for up to four years. Tigo is working with others in our industry to propose changes to the bill in order to clarify definitions and responsibilities, as well as emphasize the technical limitations facing operators in these circumstances. Like many other pieces of legislation in this space, the bill addresses removal of illegal content from websites. As an operator, though, Tigo is restricted to blocking the URL only; website domain owners are the sole arbiters of content on their sites.

In December 2019, we received guidance from the Costa Rican authorities about technical changes to interception techniques, namely the centralization of requests from judicial authorities for live surveillance related to criminal investigations on a new platform 'SOLITEL'. All such requests still require the relevant judicial authorizations, and there are no major privacy or FoE risks foreseen by the changes. Nevertheless, we are reporting this as a Major Event as it represents a significant operational change relating to surveillance techniques.

9. Trends and priorities for 2020

Trends in our operating environment

As noted previously, the number of major events in our markets decreased in 2019. Significant changes in our business over the past few years, such as exiting and consolidating various operations in Africa while expanding in Latin America, make year-to-year trend analysis difficult. We continued to receive shutdown orders in the Africa region during 2019, but our divestment from certain jurisdictions will likely contribute to a further decrease in major events during 2020. We remain alert to the numerous security issues and political challenges in countries where we operate. We will continue working with local authorities to improve transparency and accountability as well as to educate authorities about the need for proportionate action.

During a period of heightened electoral activity in Millicom's Latin American markets, we experienced only two major events in the region (see details in previous section). Given some recent election unrest across Latin America, the decrease in major events is an especially positive trend. Still, we remain alert and prepared for major events to occur in any of our markets in the future.

New proposals for laws concerning cyber security and changes related to operational procedures in surveillance—trends highlighted in our previous LED reports—represented the only major events in Latin America in 2019. These types of events are likely to continue as governments seek to understand how new technologies can help them in their national security efforts. Unfortunately, we sometimes see legislative proposals copied directly from other jurisdictions without proper consultation in a multi-stakeholder forum. Through our work with the GNI, we aim to demonstrate that this type of interaction, with all actors working on joint solutions, is the most effective way to understand and satisfy the demands and wishes of the populace as well as the governments.

Prison shutdowns remain a significant challenge in the Central America region. Although we had no major events related to this issue in 2019, signal-blocking measures in Central America continue to be a focus for industry advocacy efforts with new measures under discussion in Panama now also.

We aim to redouble our efforts with other stakeholders in civil society to continue drawing international attention to signal-blocking issues. We have discussed this topic and shared best practices with our industry peers on several occasions. We have also continued our work on this topic as a policy focus area for the GNI, and we remain encouraged by the potential of this group to help address the issue. Millicom supported the GNI in its work to produce a one-page guide for policymakers and government officials to ensure they fully understand the consequences of network shutdowns. The #KeepItOn campaign by Access Now also continues to play an important role in highlighting these events by aggregating information about shutdowns and building awareness.

Capacity of local law enforcement

Most requests we receive outside of the established legal process tend to stem from certain law enforcement officials' incomplete understanding of the laws and / or technical operations. In our view, some local law enforcement authorities also lack the capacity, resources and knowledge to understand the ICT ecosystem. This deficit, coupled with having inadequate access to the latest cyber-investigation methods, can lead to requests of our operations that we are unable to carry out or that are disproportionate to the issue the authorities are trying to address.

A common example is when authorities issue a request related to content that we do not hold, such as content on social media services like YouTube, WhatsApp or Facebook. Such data is held outside of the requesting jurisdiction, and complex mutual legal assistance treaties make its prompt retrieval difficult for local law enforcement agencies.

We meet regularly with law enforcement agencies regarding disproportionate or overreaching requests and proposals, to help educate them about the complexities involved. We always work to provide best practices from other countries where we have successfully negotiated safeguards in interception processes. Examples include independent oversight, narrow and focused orders for legitimate purposes only, strict time limits, and the ability to verify that the correct authorized individual or team is carrying out the request.

Advocating for clear laws

Clear laws and processes are crucial tools for telecommunications companies in respecting the privacy and FoE of our customers. We operate local subsidiaries that are bound by local laws—perfect or not—and we do not have the option of selecting the laws with which we will comply. Therefore, we advocate clearer laws—which respect international conventions and narrowly define who, how and under what circumstances law enforcement requests can be made—even when achieving the desired end result may require more time. We consider such clarity to be a core instrument in promoting the proportionate use of law enforcement powers. Clear laws also help us more easily assess the legality of requests, which benefits both the privacy and FoE rights of citizens. In addition, clarity helps make law enforcement processes more efficient and allows us to successfully challenge requests that do not comply with the applicable law.

We welcome additional technical assistance from the international community and other sources as we strive to include human-rights considerations in cyber-investigations. Assistance from these stakeholders also helps in designing transparent and clear laws around surveillance that incorporate international human-rights principles.

Priorities for 2020

We will continue our engagement efforts with all stakeholder groups around issues of FoE and privacy. In addition, we will further promote related internal guidance by continuously monitoring the effectiveness of our existing guidelines and procedures related to law enforcement assistance. We rolled out new guidance at a local level in late 2018, with in-person training sessions occurring at regional summits and in specific countries throughout 2019. We performed two training sessions in Panama, first with the new Cable Onda team and subsequently in a joint session with both the Cable Onda and Telefonica teams, which now work together following our acquisitions of both. We also held a similar session with new and existing employees in Nicaragua, following the acquisition of Telefonica's assets there.

We take compliance with our internal procedures very seriously and on some occasions (although rare) we have sanctioned employees who did not follow our guidelines and controls. This reflects the natural evolution of our maturity process and our robust framework for protecting privacy and FoE.

We will continue to attend major civil society events and promote the need for further safeguards on human rights in international development aid and financial assistance. We will also continue to promote the need for human rights-based technical support for legislators and law enforcement enitites in our regions. Most importantly, we will continue speaking directly with relevant government agencies whenever possible. The upcoming Rightscon event in San Jose, Costa Rica, during summer 2020 will be a valuable opportunity for multi-stakeholder discussion of key topics, with a focus on our main operating region.

We look forward to also building upon our membership in the GNI to jointly address challenges shared by this multi-stakeholder group.

We are thrilled to have successfully completed our first GNI Assessment and to be among the first telecoms operators in the world to do so. The relevance and importance of the GNI in today's environment, where FoE and privacy issues are at the forefront of human rights and security debates worldwide, cannot be overstated. Through the GNI, we have gained partners for shared learning and received crucial feedback from expert assessors on the effectiveness of our policies and processes.

Our focal points with the GNI include helping to define clear, transparent and effective surveillance laws that incorporate appropriate safeguards. As countries continue to revise their surveillance and interception-related legislation, we believe all stakeholders in this area need a clearer definition of what "good" surveillance laws look like.

During 2020, we will continue working with BSR to deploy HRIAs in select local operations. We aim to complete this process in all operations by 2021. We are learning a great deal about our risks and opportunities in the areas of human rights and FoE and privacy issues through the HRIA process. This has allowed for greater cross-pollination of best practices and standards among our local operations.

Finally, we have launched a comprehensive privacy policy framework that includes GDPR-type standards. We have launched an internal platform for employees, as well as a privacy section on our external website - which we will continue to develop so that all users can consult all our privacy-related policies and commitments along with related materials and interactive tools.