MILLICOM
THE DIGITAL LIFESTYLE

tigo

2021 Millicom Group

Law Enforcement Disclosure (LED) Report

Our purpose is to build the digital highways that connect people, improve lives and develop our communities.

What's inside this report

Contents

PAGE 1
1. Introduction

PAGE 3
2. Reporting at Millicom

PAGE 5
3. Our governance and engagement

PAGE 7
4. South America
a. Overview *page 7*
b. Legal frameworks *page 7*
c. Law enforcement requests in 2021 *page 8*

PAGE 9
5. Central America
a. Overview *page 9*
b. Legal frameworks *page 9*
c. Law enforcement requests in 2021 *page 10*

PAGE 11
6. COVID-19 requests

PAGE 12
7. Major events in 2021

PAGE 15
8. Trends and priorities for 2022

1. Introduction

Millicom's 2021 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.

FoE issues continue to grow in relevance and importance in the context of an increasingly digital and interconnected world. Since 2015, Millicom has produced an annual 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 the manner in which we manage these 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.

Our business success relies on customers' trust in us to respect their privacy and FoE, which also goes hand in hand with our duty to respect international norms as well as local laws in the countries where we operate. An ever-evolving technology landscape creates greater challenges for our sector, for governments and for law enforcement authorities around the globe. This is why we have chosen to partner with organizations such as the U.S. Chamber's Coalition for the Rule of Law in Global Markets; the Center of Studies for the Development of Telecommunications and Access to the Society of Information in Latin America (CERTAL); the CIFAL Global Network, part of the United Nations Institute for Training and Research (UNITAR); and the United States Telecommunications Training Institute (USTTI), a joint U.S. government/industry venture designed to meet the training needs of those who design, regulate and oversee the communications infrastructures of the developing world.

As our lives are increasingly digitized, and enhanced connectivity drives a greater convergence of sectors and technologies, we must work hand in hand with legislators, regulators, industry and civil society to ensure we find the right balance in answering the big questions ahead.

We must balance our respect for customers' 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 such as acts of terrorism. Whenever we face a government request for customer information, we seek to minimize the impact of that request on our customers' right to privacy and FoE. Before we respond to any legal demand, we determine that we have received the correct type of demand based on the applicable law for the type of information sought.

Moreover, when any conflict arises between a local law and the United Nations' 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.

We continually study and implement lessons learned from our industry peers and from stakeholder engagement. We hope this edition of our LED report will contribute to the constructive work among different stakeholder groups to better protect our users' privacy and FoE.

Luxembourg, February 2022

Karim Lesina

Executive Vice President, Chief External Affairs Officer

Salvador Escalón

Executive Vice President, Chief Legal and Compliance Officer

2. Reporting at Millicom

Millicom is a leading provider of fixed and mobile services dedicated to emerging markets. We operate under the Tigo brand in nine countries across Latin America. Our company serves more than 56 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.

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
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, complying with applicable laws 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 these considerations in mind, we subdivide our reporting into two regions—Central America and South America—to provide more granular and detailed information. This LED report covers law enforcement requests, major events[1] and COVID-19 requests in the Latin America region.

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' FoE and privacy.

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.

We have limited 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.

We split Latin America into Central and South America, which allows for more granularity in the numbers. We have conducted considerable internal risk analysis and debate about publishing country-specific numbers before deciding on the approach contained in this report. A major reason for our decision is that several of our countries of operation prohibit such disclosure. 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 regarding the disclosure of numbers might, in our risk/benefit assessment, lead to negative outcomes for our operations and our ability to promote more rights-respecting practices.

We have worked with our former Telecommunications Industry Dialogue (TID) peers and with the law firm Hogan Lovells to create a legal frameworks resource that details 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:

[1] While their motivations may be valid and legal and/or be in line with regulatory instruments/frameworks in a local context, 'Major Events' can include requests that contradict internationally recognized norms and commitments in the areas of Privacy and Freedom of Expression, as well as international norms more generally, such as (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, operational changes relating to surveillance techniques, 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. Reporting at Millicom–continued

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. However, we have seen increasing legislative proposals to mandate or request the take down of illegal online content in recent years. This content often is not under our control and can only be taken down by the host content provider. 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 ESG (Environment, Social and Governance) reporting process through

Enablon, a dedicated tool into which local legal teams enter total numbers 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 comprising senior staff from the functional areas of Government Relations, Regulatory, Security, and Legal, Ethics and Compliance. ERM Certification and Verification Services (ERM CVS) has assessed Millicom's numerical information related to law enforcement demands as part of our ESG reporting limited assurance process, as disclosed in our Annual Report on page 42.

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. See 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 industry, 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 monitoring the effectiveness of Millicom guidelines, adding controls and improving the readiness of local and global teams to handle any major events, along with 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.

We continuously review and strengthen our existing policy framework created in 2015, making updates in line with technological advancements, emerging standards and best practices, and evolving political and security environments in our operations. Finally, our **Global Privacy Policy** addresses customers' privacy rights.

Human rights impact and risk

In 2017, we carried out an initial 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 Verisk Maplecroft's risk indices.[2]

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 opportunities to improve.

Millicom's 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. Therefore 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 our South American operations in 2019. We have continued to roll out this assessment across our operations in Central America during 2020-21. We included an executive summary of the results from South America in last year's report.

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

Governance and oversight of human rights

Millicom's Board of Directors (BoD) and our Executive Team (ET), which includes the EVP Chief External Affairs Officer, oversee our ESG strategy and activities. Millicom's ESG Committee is chaired by the CEO and the Board receives regular updates on ESG topics, with Millicom's CEO, EVP Chief External Affairs Officer and EVP Chief Legal and Compliance Officer attending the BoD meetings. The EVP Chief External Affairs Officer also reports to the ET on a monthly basis, while Millicom's External Affairs team is responsible for ongoing management of human rights issues in the company.

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. It includes the EVP Chief Legal and Compliance Officer, VP Ethics and Compliance, Chief Information Security Officer, VP General Counsel Corporate and Global Chief Privacy Officer, and our Political Relations and 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 several times in 2021 to review risks and actions related to FoE and privacy. These meetings provided an opportunity to brief new team members on our ongoing work on these issues, as well as to help 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.

We completed our **Global Privacy Policy** framework in 2018 and have continued to execute it during the past few years. 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** and Tigo Privacy Notices, including how we use, process and secure customer data. Our websites also provide channels and contact points for our customers to raise concerns about our policy or their privacy.

Our EVP Chief External Affairs Officer, VP Ethics and Compliance, EVP Chief

[2] https://maplecroft.com

3. Our governance and engagement–continued

Technology and Information Officer, EVP Chief Legal and Compliance Officer, VP General Counsel Corporate and Global Chief Privacy Officer 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 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 was a founding member of the Telecommunications Industry Dialogue (TID) on Freedom of Expression and Privacy. In 2021, we joined the Rule of Law Global Coalition, part of the U.S. Chamber of Commerce. We also joined CERTAL, an organization focused on FoE issues in Latin America. We 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 technology landscape. During 2021, we developed and expanded our relationships with civil society actors via various events such as the United Nations' VI Regional Forum on Business and Human Rights for Latin America and the Caribbean and the Organization for Economic Co-operation and Development's (OECD) "Driving a New Social Contract for Latin America." 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. We also seek to highlight risks from disproportionate government action, especially to governments' reputation and foreign investment possibilities, and 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 technology 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 training on these topics with our local staff at regional summits as well as through specific training sessions 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.**

Millicom's main policy framework for law enforcement requests is the **Group Guidelines for Law Enforcement Assistance (LEA) and Major Events,** which summarize:

- Our obligations within international standards and 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 these guidelines is available at https://www.millicom.com/ media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf.

We review and revise these guidelines on an ongoing basis. We also consistently train our staff on implementation and developments.

Our **internal control process** assesses how well our local operations apply and comply with various global policies and controls. These controls verify 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 controls also aim to limit and make 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. These guidelines define steps to take in 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 2021, we built on previous work assessing how to streamline communication of these internal policies, guidelines and controls to our local staff.

Information security

Millicom, as well as all Tigo operations, protects our networks and customers as one of our highest priorities. Millicom has a dedicated Global Information Security team that oversees the strategy and direction of all security-related activities across the enterprise. Our global information security program provides policies and standards, vulnerability management and third-party risk management. The team also oversees implementation of technical solutions across the company. Millicom's BoD receives regular reports on new and evolving risks and technology initiatives. Since we operate in many countries around the world, developing a risk framework that can address the various legal and regulatory reporting needs, as well as the unique challenges individual countries face, is paramount. Millicom has implemented a risk framework that is based on a combination of the NIST Cybersecurity Framework (CSF) as well as the ISO/IEC 27001:2013. This blended approach allows each country to address local regulators in whichever format they prefer while also providing a common risk and maturity measurement across our entire enterprise.

4. South America

Overview

Millicom has operated communications networks in South America for close to 30 years now. 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 2021, we invested a total of US $1.1 billion in the South America and Central America regions to further develop our mobile and fixed communications networks. These investments ensure better bandwidth 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[3] and the employment and services we provide. For more details, see the tables to the right.

Table 2
South America (Bolivia, Colombia and Paraguay)

Total B2C mobile customers ’000	Customer relationships[4] ’000	MFS customers ’000
18,278	2,967	2,757

Table 3

Country	B2C mobile customers ’000	Workforce[5]	Population[6] ’000
Bolivia	3,948	2,535	11,670
Colombia	10,803	4,224	50,880
Paraguay	3,528	4,584	7,133

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 long-lasting internal conflicts and the war on drugs, the processes are significantly more complex. However, 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. However, interception procedures are not active yet as we are still awaiting operational regulations to manage these processes. We have regular discussions with authorities regarding the implementation of such interception techniques.

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 that is 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 by 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 the legality of these requests before providing authorities with the requested information.

[3] See page 119 in our Annual Report.
[4] Total number of households with an active service.
[5] Workforce accounts for employees directly employed by Millicom.
[6] Population statistics as per World Bank 2020.

Law enforcement requests in 2021

Table 5 shows an increase in requests received from law enforcement authorities across our markets in South America. This reflects an increased level of both criminal and law enforcement activity as countries exited strict lockdowns during 2021 as a result of COVID-19.

As previously noted, a number of countries in the region (including Colombia and Paraguay in South America) 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 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 and 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 2021 was 0.112%.

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	Military, 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
2021	798	298	23,758	0.112%
2020	749	177	19,333	0.110%
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%

5. Central America

Overview

Millicom has operated in the Central America region for close to 30 years. We provide a wide range of services—including high-speed data, cable TV, voice and SMS, Mobile Financial Services (MFS) and business solutions—in six different markets.

During 2021, Millicom invested a total of US $1.1 billion in the South America and Central America regions to further develop our mobile and fixed communications networks.

These investments ensure better bandwidth 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[7] and the employment and services we provide.

We are now reporting across our entire footprint in the region (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Panama) after several acquisitions in recent years. 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. We also completed the takeover of Cable Onda and Telefonica's assets in Panama in December 2018 and September 2019 respectively. All numbers related to these businesses are now fully included in our reporting.

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 operate fixed networks only, the number of law enforcement requests is significantly lower than in other Central American markets.

Table 6

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

Total B2C mobile customers '000	Customer relationships[8] '000	MFS customers '000
24,795	1,925	2,853

Table 7

Country	B2C mobile customers '000	Workforce[9]	Population[10] '000
Costa Rica	N/A[11]	469	5,094
El Salvador	2,795	632	6,486
Guatemala	11,424	3,133	16,860
Nicaragua	3,653	423	6,625
Honduras	4,927	938	9,905
Panama	1,997	2,536	4,315

[7] See page 119 in our Annual Report.
[8] Total number of households with an active service.
[9] Workforce accounts for employees directly employed by Millicom.
[10] Population statistics as per World Bank 2020.
[11] Millicom does not have mobile operations in Costa Rica but is the market leader in B2C home and B2B services.

5. Central America–continued

In Honduras and El Salvador, the law mandates direct access to our networks by 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 and Panama, interception also takes place under judicial orders, which we receive and review before opening the line for the specified time period. In Nicaragua, there is no live interception system in place. For customer metadata, judicial orders from the same courts are required in all 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 the 'Major events' section of this report 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 2021

Law enforcement authorities across our markets in Central America continue to tackle crime and violence in the region. Some of these countries rank among the most violent in the world. 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 from organized crime. Differences in the populations of our Central American and South American markets add to the difficulty of making direct comparisons from one region to the other. 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 gradually increased over the years. This year the increase is largely due to the aforementioned reasons linked to COVID-19. That said, recent acquisitions make direct comparisons to previous years difficult. Certain requests may involve a large number of metadata records, which can skew the numbers. In Central America, the percentage of metadata requests received per customer in 2021 was 0.1%.

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
Nicaragua	Criminal Courts, Prosecutor's Office, Police, Financial Analysis Office, TELCOR	Judges in Criminal Courts, Attorney General, Director General of TELCOR
Panama	Attorney General's Office	Judicial branch

Table 9

Central America	Interception	MFS	Metadata	Metadata requests per customer
2021	1,847	301	26,418	0.100%
2020	1,555	323	14,870	0.058%
2019	1,389	275	12,633	0.072%
2018	1,533	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%

6. COVID-19 requests

Since 2020, we have decided to include a specific section in this report related to COVID-19, given the pertinence of the topic and its related impact on our law enforcement engagement.

Types of requests related to COVID-19

We continued to witness a wide range of requests from governments to help address public health challenges related to COVID-19 (see Table 10 for details). As per the previous year, these predominantly included push SMS notifications and the use of media and advertising space for public health messaging. Other requests for support in efforts related to contact-tracing and identification of vulnerable populations for distribution of relief funds were much less common during 2021 than the previous 12 months, as responses to COVID-19 by governments evolved. Although the objectives and motives behind many of these request types remain logical, pragmatic and understandable, we still feel compelled to push back in circumstances where we believe protections for the privacy and security of our customers could be undermined in the long term.

These have not been easy decisions, and we often risk damaging relations with our stakeholders in government who are desperately seeking solutions to address a crisis like no other experienced in our lifetime. We have offered our services and support in many other ways—for example, by using our Mobile Financial Services platform to distribute funds to vulnerable populations—but we could not agree to providing our customer database to other governments that needed to correctly identify which parts of the population needed such funds most urgently. We hope that this information helps provide some detail on these types of challenges and will improve understanding of the types of situations faced during this pandemic.

Table 10
Latam Request Count 2020–2021

Request Type	Number of requests
Free SMS	164
Materials, supplies, devices, donations	40
Other (URL Access, combo telecommunication Services, Unique Request/Services)	36
Free access to government or public webpages	32
Free advertising space on Tigo networks	23
Free voice/minutes	21
Free WiFi/Internet	20
Free data	19
Monetary donations	15
Free access to Government run phone numbers	10
Sponsorship/gift	12
Free MFS transactions	7
Man hours/Labor services	4
Free land line services	4
Free cable	3
Geolocation	2
Use of Millicom websites, points of sale, and SMS to promote health messages on behalf of Government	1
TOTAL	**413**

7. Major events in 2021

Major events are requests that fall outside 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 2021.

Deciding whether to challenge a major event is rarely simple. These requests or decisions 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, geographic 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[12]
- 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 2021, we recorded eight major events, a decrease compared with 2020, as shown in Table 11. Four occurred in South America, while three were 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.

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 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 geographic 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 that are ongoing with no significant changes in terms of obligations or requirements, we do not count this as an additional event. For 2021, we recorded no major events in this area. Although we do not report ongoing signal blocking in prisons (or new blocking measures that 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 our work 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 often unable to describe how we reduce the impact of these events on our customers' privacy or FoE, given the sensitivities around what are sometimes ongoing investigations or national security incidents.

Table 11
Type of major event

	2015	2016	2017	2018	2019	2020	2021
Shutdown or restriction of services	8	8	2	7	8	8	2
Proposal for significant changes in local laws	3	5	4	5	1	2	3
Proposal for significant changes in technical or operational procedures	3	2	1	2	1	0	2
Disproportionate customer data or interception requests	2	1	2	2	0	3	0
Politically motivated messages	2	1	0	1	0	0	0
Other	2	1	5	3	0	2	1
TOTAL	**20**	**18**	**14**	**20**	**10**	**15**	**8**

[12] 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.

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 are adequately informed and 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. Regardless, we continue to cooperate with the authorities to address ongoing concerns in this area. Costa Rica also introduced new signal-blocking measures in 2018, but we do not have mobile operations in the country. We have assisted with monitoring and advocacy work performed by organizations such as the GSMA and ASIET and will continue working with these organizations on these topics.

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.

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 authorized 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 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 to monitor progress and the functioning of jammers in prisons. Operators are also donating additional equipment to monitor and locate devices within prisons.

[13] https://qz.com/africa/1923616/tanzanias-magufuli-blocks-twitter-facebook-sms-on-election-eve/

Honduras

In 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 have been disputing these sanctions in the courts over the last few years, and in 2021 Tigo asked CONATEL to void the various sanctioning processes for alleged prison calls due to inconsistencies in these cases. CONATEL issued a positive resolution to our requests on 2 December 2021, closing these administrative processes definitively.

Disproportionate customer data or interception requests

As outlined in the previous section on COVID-19 requests, we experienced some extraordinary requests related to efforts to address the public health crisis. These included requests from certain governments to access our customer databases to better understand their populations and distribute relief funds more effectively. In Colombia, a request like this was received from DANE, the government's statistical agency, by all major operators via the local Telecoms Chamber Asomovil.

We sent a letter to DANE as a member of Asomovil and GSMA, and separately as Tigo, outlining our reasons for not complying with this request. These included privacy concerns and DANE's lack of legal jurisdiction for requesting the data. DANE responded by reiterating the need to comply, but we remained steadfast in not providing this information.

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. 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.

Colombia

The Colombian government proposed a bill in Congress (PL #600) aimed at child protection measures. The bill sought to create an "expert" commission to provide an index of forbidden content to be blocked by all media, including internet, but with such broad discretion that it could potentially be used to block any content creator.

The bill was eventually retracted by the government after strong criticism from civil society and the private sector.

Paraguay

A bill was introduced in Congress establishing biometric registry for the identification of mobile telephony users.

This bill is similar in nature to the one approved, and eventually vetoed, by the President in 2017.

The bill would require biometric registration of mobile telephony activations and operators would have to run a system to keep track of service activation requests throughout the country in real time. The biometric information requirements include the customers blood group and driver's license details.

The bill also contemplates the blocking of telephony lines by the National Police and Public Ministry if registration is not completed.

Via the local telecoms chamber, Tigo is arguing that blocking access to communications should be an exceptional measure, and the requirements of due process cannot be ignored, such as the order of a competent judge. The bill is still being studied within various commissions of the Congress and has not yet been discussed in the plenary.

In October 2021, the regulator in Paraguay also issued a modification to the telecoms consumer protection bill which allows for the blocking of fraudulent telephony lines. The blocking requests must come from the Minister of the Interior and can last for up to 72 hours only. The Telecoms Chamber appealed against the original version of the proposal, aiming to reduce the impact and scope. A new version of the bill was subsequently issued in December 2021.

8. Trends and priorities for 2022

Trends in our operating environment

As noted previously, the number of law enforcement requests in our markets increased in 2021 as strict lockdown rules were relaxed. Major events decreased, but 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 remain alert to numerous security issues and political challenges in countries where we operate. We continue working with local authorities to improve transparency and accountability as well as to educate authorities about the need for proportionate action.

New frameworks concerning cybercrime and content regulation—trends highlighted in our previous LED reports—continued to emerge. These types of events are likely to increase 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. Via our regional associations such as ASIET and GSMA, 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 recent years, signal-blocking measures in Central America continue to be a focus for industry advocacy efforts.

We aim to redouble our efforts with stakeholders 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.

Capacity of local law enforcement

Most requests we receive outside of established legal processes tend to stem from a misunderstanding by certain actors 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 inadequate access to the latest cyber-investigation methods, can lead to requests 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 agencies 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 for telecommunications companies in respecting the privacy and FoE of our customers. We operate local subsidiaries that are bound by local laws and do not have the option of selecting the laws with which we will comply. Therefore, we advocate for 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.

It is for this reason we have joined USTTI, a nonprofit, U.S. government/industry joint venture designed to meet the training needs of the women and men who design, regulate and oversee the communications infrastructures of the developing world. Since 1982, USTTI has graduated communications officials, regulators and entrepreneurs from 177 developing countries. We hope to work closely with this organization to help construct a positive dialogue on transparent, agile and robust processes for government requests that protect our customers’ human rights.

8. Trends and priorities for 2022–continued

Priorities for 2022

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 continue to review and update our guidance to local operations in 2021. We also performed specific training sessions on LED and human rights issues in Nicaragua and Costa Rica.

We take compliance with our internal procedures seriously. On rare occasions we have sanctioned employees who did not follow our guidelines and controls. This reflects the natural evolution of our maturity process, our robust framework for protecting privacy and FoE, and our employees' awareness of the materiality of these issues.

We 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 also continue to promote the need for human rights-based technical support for legislators and law enforcement entities in our regions. Most importantly, we continue speaking directly with relevant government agencies whenever possible.

We look forward to building upon our multi-stakeholder interactions to continue our important work on FoE and privacy issues, which remain at the forefront of human rights and security debates worldwide. Through multi-stakeholder dialogue, 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 external actors 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 2022, we will continue to deploy HRIAs in select local operations. We are learning a great deal about our risks and opportunities in the areas of human rights, FoE and privacy 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 privacy policy framework in accordance with applicable laws and an internal platform for employees. We also launched a privacy section on our external website, which we will continue to develop so that all users can consult our privacy-related policies and commitments, along with related materials and interactive tools.