MILLICOM
THE DIGITAL LIFESTYLE

2018 Millicom Group Law Enforcement Disclosure (LED) Report

We believe in better.
We believe in tigo

What's inside this report...

Contents

1. Introduction

This is Millicom's fourth Law Enforcement Disclosure (LED) report, covering the year 2018. It serves to provide information about the extent and context of our interaction with law enforcement agencies and governments related to issues that affect the privacy or freedom of expression of our customers in Latin America and Africa.

In today's increasingly digital world, privacy and freedom of expression (FoE) are at the forefront of human rights debates. During 2018, the European Union's (EU) General Data Protection Regulation (GDPR) established itself as an emerging global standard on data protection and privacy while concurrently significant data and privacy breaches involving major internet companies have led to increased focus on the importance of personal data security.

For Millicom, recognizing the importance of our customer's privacy and FoE rights came early. In 2013 Millicom became a founding member of the Telecommunications Industry Dialogue (TID)- a group of telecom operators focusing on privacy and FoE issues. Since merging with the Global Network Initiative (GNI) in March 2017, the latter organization has grown to over 60 participants, bringing together technology companies, ethical investors, academics and human rights organizations. They work jointly on solutions to complex situations in which people's fundamental rights for privacy and free expression come into conflict with government measures to protect national security.

The ever-evolving technological landscape in which we operate has created increasing challenges for government and law enforcement authorities. Globally, security agencies keep pushing governments to place greater obligations on technology firms to ensure public safety. Established methods and practices for information requests related to criminal investigations are becoming outdated. We see this reality in calls by the so-called "Five Eyes" intelligence alliance (including Australia, USA, Britain, Canada and New Zealand) for technology firms to weaken encryption or face legislation compelling them to create backdoors into their systems. The phenomenon of 'Fake News' or disinformation campaigns via social media, with tangible impacts on electoral events, serves as another example of the challenges emanating from a hyper-connected world.

This increasingly complex landscape played a key role in Millicom's decision to join the GNI. We firmly believe that positive outcomes for human rights will require collaboration based on appreciation of the full spectrum of considerations and realities—something that can only be achieved when all concerned stakeholder groups come together. Through the GNI, we have gained further partners for learning, received crucial feedback from expert assessors on our processes and policies, and can now act as a powerful and strong voice on these issues. All of this helps us to minimize human rights implications of the demands we receive from governments, while helping us to continue to build trust with our customers in terms of respecting their privacy and FoE rights.

At the same time, as we consistently emphasize, we recognize that our respect for our customers' human rights must go hand-in-hand 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 crime or 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 between local law and the Universal Declaration of Human Rights and other international human rights standards arise, we strive to resolve that conflict in a manner which respects the right to privacy and freedom of expression, as well as the fundamental right to access the internet and/or communications services.

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 on how we handle government requests for their data, the challenges we face from time to time in dealing with government request and how we manage such challenges.[1] In this report, we also set out our ongoing commitment and progress in the areas of privacy and FoE, how our operations impact human rights more generally, and how we work independently and with others to minimize potential negative impacts.

Luxembourg, February 2019

Rachel Samrén
Executive Vice President Chief External Affairs Officer

Salvador Escalón
Executive Vice President and General Counsel

[1] Note: We now also issue this report in Spanish, and have done so since 2017—in line with our significant business focus on the LatAm region.

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, as well as the Cable Onda brand in Panama, and two countries in Africa (including the Zantel brand in Tanzania). We set the pace when it comes to providing high-speed broadband and innovative services under our trademark The Digital Lifestyle® to more than 50 million customers. 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 the first choice for customers in all our markets. Millicom's shares are listed on Nasdaq Stockholm in the form of Swedish Depository Receipts and on the Nasdaq Stock Market in the US as from January 9, 2019.

Millicom's two key motivations for publishing this latest LED report have not changed since we published our first LED report in 2015: (1) Respond to stakeholders who have asked us to be more transparent about how we deal with government requests, and (2) Advance the understanding of 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 high levels of transparency and protecting our staff and assets on the ground. In many markets where we operate, we are legally prohibited from disclosing law enforcement assistance requests. In other instances, disclosure may place the safety of our staff and assets at risk. With this in mind, we report on a regional basis with Latin America subdivided into two regions - Central and South America - to provide more granular and detailed information about law enforcement requests. We also continually study and implement lessons learned from our industry peers and civil society resources, predominantly through our association with the Global Network Initiative (GNI).[2]

We hope that the fourth edition of this report will build on and contribute to existing constructive work between different stakeholder groups to better protect freedom of expression and privacy of individuals.

What we are reporting

In this report, we disclose the type, and number of law enforcement requests we receive. More importantly, in our opinion, we also describe the overall context and trends in the demands we receive. Context matters for specific and more significant cases - what we call 'Major Events'[3] - as it highlights some very practical challenges that we encounter in our interactions with law enforcement authorities.

In this report, we also describe several of the 'Major Events' we have faced during the year. Whenever possible, we disclose the countries in which they took place.

We also disclose information about our internal policies, processes and controls that we have in place to protect our customers' privacy when we handle law enforcement requests, and how we seek to minimize effects on our customers' freedom of expression and privacy in 'Major Events'.

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

In addition, we also include information about the different types of communications services provided in each country as well as numbers of customers and our market position. These affect the number of requests we receive and should be taken into account when trying to determine the extent of government activities.

What we are not reporting

Law enforcement demands are, by definition, 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.

Discussion of sweeping national security and surveillance powers aside, requests from law enforcement come with strict confidentiality requirements which mean that often we are prohibited by law from disclosing details of the requests we receive. In some situations, we may be explicitly required by law not to disclose any details of the request, and failure to comply with these requirements could lead to severe penalties for our company and our local staff (including possible imprisonment).

It is also often difficult for us to discuss publicly how we engage with law enforcement or other authorities when we receive requests or the ways in which we challenge their approach. Doing so would most certainly affect our ability to engage in the future, and could, in some cases, put personnel at risk. This is a source of frustration at times, as it may lead to incorrect perceptions of inaction on our part. This is also why, for the most part, this report describes our engagement in broader terms rather than specific events.

Unlike some of our peers, we do not disclose the numbers of government requests by country. The reasons for this are multiple. Disclosure in certain countries is legally prohibited. Only in Tanzania does the law explicitly state that we can publish aggregate numbers of requests received. In the remaining countries, the law is either not clear as to whether we can publish the numbers of requests received, or it explicitly prohibits publication.

[2] In editions previous to the 2017 LED report, we have reported our progress based on the Telecommunications Industry Dialogue (TID) principles. Since we subsequently joined the Global Network Initiative (GNI), we will no longer be reporting against the TID principles. Instead, we will now report against the GNI principles, following our first assessment process by the GNI which is due to close in March 2019.

[3] 'Major Events' can include clearly politically motivated requests for (but not limited to): shut down 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.

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 highly likely to put the safety of our employees at risk. This is not necessarily always a risk from government but can equally be from criminal entities whom the requests concern. In some countries, even beginning discussions with authorities regarding disclosing numbers might in our risk/benefit assessment lead to negative outcomes for our operations and ability to promote more rights-respecting practices.

For these reasons, we have taken the decision to aggregate numbers of requests on 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 together with our former peers within the Telecommunications Industry Dialogue (TID) and with the law firm Hogan Lovells to create a legal frameworks resource[4] detailing the legal frameworks governing government surveillance powers in our markets. For this reason, we are not outlining specific laws by country in this report, as these are already covered in the legal frameworks resource in much more detail.

Definitions of different types of requests

There are no agreed upon definitions or ways to classify law enforcement requests across the Information, Communications and Technology (ICT) industry. Standardizing definitions is challenging given the multiple jurisdictions and business models in our wider sector. At Millicom, we classify requests received into three distinct categories: requests for 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 represent the great majority of requests we receive on a daily basis. We report all other types of requests, which fall outside of the definitions below, as 'Major Events'. We do not report on content take-down requests specifically as these are relatively rare in our markets, with the exception of legally mandated removal of access to child sexual abuse content in Colombia. That said, we have noted an increasing number of requests for take-down of online content in recent years (often content that we do not control and which can only be taken down by the host content provider) and we are also seeing various legislative proposals seeking to mandate the removal of 'illegal' content online. Such proposals are accounted for 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 of each of our local operations. As prescribed in our '**Law Enforcement Assistance and Major Events Guidelines'**, these legal departments are charged with receiving and reviewing all demands for their legality before being executed. They log each demand by date, type (see Table 1), and requesting authority. When requests are legally justified, these same teams provide the requested information to the authorities.

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

Information related to 'Major Events' is reported according to an escalation mechanism defined in Millicom's **'Law Enforcement Assistance and Major Events Guidelines'**. 'Major Events' are reported by our local CEOs or other local senior management to a specific small group of senior regional and global staff.

Information about 'Major Events' is collected throughout the year and the Global External Affairs team maintains a log of them. We are confident that all 'Major Events' are now escalated to the Group, to our cross-functional Law Enforcement Disclosure (LED) Committee, comprised of senior staff from the External Affairs, Legal, Security, and Compliance functions. This has been a significant step since the installation of our 'Major Events' process and LED Committee back in 2015.

This is the third year that the numerical information relating to law enforcement demands was externally assessed within our corporate responsibility reporting limited assurance process carried out by Ernst & Young (EY) as disclosed in our Annual Report on pages 207 – 209 (limited assurance report).

Table 1
Definitions for the three categories of requests

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

Feedback

We are keen to hear from, or work with, anyone who wants to promote open access and transparent and accountable processes for surveillance and security. We also welcome feedback on this report or on these issues in general. Please contact CR@millicom.com or find our full contact details on our website.[5]

[4] Since joining the GNI, this resource has been migrated to the following website: https://globalnetworkinitiative.org/legalframeworks
[5] https://www.millicom.com/

3. Our internal policies, guidelines, and governance

Millicom recognized at an early stage the need to engage proactively on privacy and freedom of expression, to understand human rights risk related to our operations and to put in place processes to manage them.

We have taken several steps to minimize our risks where we can, introducing and updating Group guidelines, adding controls and improving the readiness of global and local teams to handle any 'Major Events' and the human rights and reputational issues they pose. We initially focused on improving local processes by providing support to local management and the teams who manage law enforcement relationships. Since then, we have significantly progressed on this journey, instilling a culture of respect for privacy and FoE rights throughout our business and acting as a leader in emerging markets on these topics.

In 2018, during our first year of external GNI Assessment, we reviewed and strengthened our existing policy framework, originally created in 2015. This work largely revolved around streamlining and consolidating all our previous work over the last few years in this area, making updates in line with technological advancements and an evolving political/security environment in some of our operations. Millicom has also recently adopted a **Global Privacy Policy,** based on GDPR requirements, which addresses, among other topics, its customers' privacy rights.

Human Rights Impact and Risk

In 2017, the first year of our membership in the GNI, 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. The salient and material risks posed by each country were derived from VeriskMaplecroft's risk indices.[6]

As part of this risk assessment, we engaged external expert support to pull together all our current resources and learnings so that we better understand our potential risks and the opportunities to improve our policies and processes.

Our significant on-the-ground presence in our markets means that we often have a strong understanding of potential risk situations and risk levels related to specific situations. We nevertheless wanted to formalize this assessment and broaden our analysis by interacting with external stakeholder groups to create a dynamic tool to update and consult on a regular basis. Therefore, during 2018, we worked with leading sustainability firm Business for Social Responsibility (BSR) to build a Human Rights Impact Assessment (HRIA) toolkit which we will deploy in select local operations as a pilot during 2019.

BSR also supported us in our Materiality Assessment, convening internal and external stakeholder interviews to help define Millicom's priorities in the Corporate Responsibility space. Naturally, privacy and FoE was a key area of focus during this assessment.

Governance and oversight of human rights

Corporate Responsibility is one of the component functions of the External Affairs team at Millicom. All corporate responsibility activities in Millicom are overseen by our Board of Directors (BoD) as well as our Executive Committee (EC) of which the EVP Chief External Affairs Officer is a member. The Board of Directors 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 EC on these topics on a monthly basis, while Millicom's Corporate Responsibility Director is responsible for the ongoing management of human rights issues in the company.

Millicom's BoD receives periodic updates on human rights issues and has directed management to continue its strong proactive approach, deepening relationships with civil society at the country level. In 2016 and 2017, the BoD received an updated human rights risk assessment relating to privacy and freedom of expression. In 2018, Millicom's Board of Directors received updates on the company's implementation of the GNI Principles and its management of risks relating to the privacy and freedom of expression from the company's EVP Chief External Affairs Officer. Millicom's Compliance and Business Conduct Committee of the Board of Directors also provided additional oversight on these issues.

Back in January 2014, when Millicom began its escalation process for government requests, the cross-functional Lawful Interception Policy Committee (LIP Committee), which has since been renamed the Law Enforcement Disclosure Committee (LED Committee), was established to better coordinate risk management. This Committee is chaired by the EVP Chief External Affairs Officer, and includes participation by the Director of Corporate Responsibility, EVP General Counsel, EVP Chief Ethics and Compliance Officer, Chief Information Security Officer, VP Legal Latam and Chief Privacy Officer, VP of Global Investigations and Regulatory Affairs Directors. The Group members prepare and jointly approve policies and processes, review our **'Law Enforcement Assistance and Major Events Guidelines'** and arising risks, and approve Millicom's reporting and engagement relating to privacy and freedom of expression. The LED Committee

[6] https://maplecroft.com/

communicates frequently and met face-to-face twice in 2018 to review risks and actions related to freedom of expression 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.

In 2018, we completed our global privacy policy framework. In addition to our **Global Privacy Policy**, Millicom's EC approved broad privacy principles, guidelines and commitments for the company, and supporting decision-making materials were created for commercial teams on customer privacy issues. The work continues to bring more transparency to Millicom's privacy policies and practices.

The privacy framework development is monitored by a steering committee consisting of four of Millicom's EC members (EVP Chief External Affairs Officer, EVP Ethics and Compliance Officer, EVP Chief Technology and Information Officer and EVP General Counsel). We will be rolling out this framework internally and externally during 2019, including the completion of Millicom's privacy commitments and guiding principles. All relevant information will be held on an online privacy policy portal on the Millicom website.

Policies, guidelines and controls

Our commitment to the International Bill of Human Rights and the UN Guiding Principles on Business and Human Rights was included in the **Millicom Code of Conduct** (2015 version) and also in the updated **Millicom Code of Conduct** (2017 version).

In addition, Millicom's commitment to implement the 'Principles on Freedom of Expression and Privacy for the Telecommunications sector' as defined by the Telecommunications Industry Dialogue (TID) was based on its membership in the TID. The TID Principles called on us to publicly report on how we are putting the principles into practice. Millicom's LED reports began as a public account of this commitment. As we are now members of the GNI, we adhere to the GNI Principles on Freedom of Expression and Privacy. We will be reporting more extensively on these commitments following our first assessment process with the GNI which started towards the end of 2018 and which is scheduled to conclude in March 2019.

During 2018, the LED Committee finalized and approved updates to **Millicom's Group Guidelines for Law Enforcement Assistance (LEA) and Major Events**. These are a streamlined, consolidated version of all our various internal policies and work we have undertaken in this area since the creation of our first set of **Law Enforcement Assistance Requests Guidelines** and **Major Events Guidelines** (by the then LIP Committee) in Q1 2015. These guidelines clearly outline 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, and how to deliver the information safely. A shortened version of this guideline is available publicly on our website.[7]

Millicom 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 its senior management team. The EVPs Chief External Affairs Officer and General Counsel working with senior members of the Corporate Responsibility and Compliance teams and are ultimately responsible for the company's implementation of the GNI Principles in relation to the rights to privacy and free expression, respectively.

Our **internal control process** assesses how well our local operations apply and comply with different global policies and controls. Two controls related to the implementation of the original LEA Guidelines were added in the Millicom Internal Control Manual in 2015. 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') to these controls on an annual basis. First assessments were carried out in 2015. Over subsequent assessments we have witnessed all operations making substantial improvements in the maturity level of their controls for the LEA guidelines. In 2018, all operations achieved one of the two highest maturity levels, meaning that 100 percent of our operations have an acceptable level of controls implemented at a local level. In 2019, we will be revising our internal control processes in line with changes made to our policies concerning freedom of expression and privacy.

'Major Events Guidelines' were approved by the LED Committee in Q3 2015. These guidelines define steps to take in the case of a 'Major Event' and an escalation process to regional and global level. The Guideline also provided practical suggestions on how to engage with the authorities to limit the remit and/or timeframe of any 'Major Event'. In 2017, we began an assessment of how we can

[7] https://www.millicom.com/media/3613/law-enforcement-assistance-and-major-events-guidelines.pdf

better 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, streamlined document now called the **'Law Enforcement Assistance and Major Events Guidelines'**. We did this to ensure our internal resources are easily understood and to ensure that they remain relevant in an ever-evolving environment.

Information security

Millicom **Information Security Standards** (ISS) address specific security requirements for customer and employee data. The ISS was published in April 2015, and came into effect in July of the same year.

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 a mandatory training for all employees. IS awareness materials are also distributed to all employees at least annually.

4. Our engagement

Millicom continues to work proactively with a wide range of actors to mitigate human rights impacts risks related to law enforcement requests. We were a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy and in 2017, we joined the Global Network Initiative (GNI) as full members, having spent 2016 as observer members. We have also engaged with many international organizations, taking part in various events (such as RightsCon and the UNESCO colloquium "Improving the communications and information ecosystem to protect the integrity of elections") and contributing to the ongoing debate around freedom of expression and privacy, as it evolves 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 2018, actively participating in the Policy and Learning Committees to further mutual interests in the defense of freedom of expression and privacy rights. During 2018, Millicom was also nominated to act as the Co-Chair of the GNI's Learning Committee, representing the company constituency.

Concurrently, we engage directly with governments and other in-country stakeholders on the topic as much as possible. We also seek to enhance governments' understanding of our obligations outside of their countries, while repeatedly highlighting the risks from disproportionate government action, especially to their reputation and foreign investment possibilities. We also discuss these topics regularly with relevant diplomatic representatives. Similar conversations and trainings occur internally with our local staff who engage with these issues on the ground.

A rapidly changing technological environment and high public-security demands can make for a difficult decision-making process as we strive to adhere to legal obligations and protect the freedom of expression and privacy of users. We provide yearly face-to-face group training on these topics with our local staff at regional summits, while constant engagement occurs internally on these issues on an ongoing basis.

Global Network Initiative (GNI)

At Millicom, we believe that our ability to shape smart legislation or appropriately challenge 'Major Events' is greatly increased by working jointly with others. In 2017, we became a full member of the GNI and active participant in its committee and policy work, sharing best practices on conducting human rights due diligence and working together on a new GNI Assessment Toolkit, expanded to address a wider range of ICT sector companies. We have also participated in many sessions and work in policy focus areas such as Internet shutdowns, intermediary liability and direct access.

During 2018, Millicom underwent its first-ever GNI Assessment by an expert external law firm focused on Corporate Responsibility practices and human rights. Millicom completed a self-assessment of its processes, practices and governance framework, as well as submitting various case studies to illustrate how we deal with privacy and freedom of expression issues in real-life scenarios. Several members of Millicom's senior management team and local Tigo operations were interviewed during this process and the assessor will present its findings to the GNI Board in March 2019. Millicom's commitment to the GNI Principles will be determined during this meeting and we will report on our assessment experience and the outcome once this process has closed.

Millicom welcomes the continued collaboration and further capacity it has secured as a full member of the GNI, with a unique multi-stakeholder forum providing the basis for collaboration and promoting positive change in relation to human rights issues within the ICT sector. We look forward to increased interaction and shared learning within the GNI, which provides a valuable forum for discussion on these issues.

UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye

Millicom highly values its continued engagement with the United Nations Special Rapporteur (SR) on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye. For the past few years, Millicom has met with UN SR David Kaye at Rightscon, where the SR typically previews his upcoming report to the UN Human Rights Council.

The Special Rapporteur's latest report was the first-ever UN report that examines the regulation of user-general online content. Millicom has helped provide input to the SR's work at previous consultations in Geneva as well as at a 'brainstorming session' with the SR held by Article 19 in London. Millicom continues to engage with the SR on his upcoming work, in collaboration with the GNI.

UNICEF

In 2018, Millicom announced the renewal of a three-year partnership with UNICEF to address child and adolescent rights. As part of this partnership, Millicom and UNICEF had previously developed a toolkit—MOCRIA (Mobile Operators Child Rights Impact Assessment)—focused on the potential impacts that technology could have on children and adolescents. The intersection of the topics of Privacy and Freedom of Expression with child rights is an area in which we are taking a leading role. Since 2017, Millicom has implemented MOCRIA in local operations and has focused on ways to improve practices around children. The widely acclaimed MOCRIA tool is available to all operators.

During 2018, Millicom and UNICEF worked jointly to design and plan the focus of our coming years of collaboration, including defining key areas of work, both from the global level where the partnership is moving towards better understanding the impact and the relationship of technology and Child Rights, as well as from a local perspective where a number of Millicom's operations actively engage with UNICEF's country offices in the execution of Child Rights focused projects and programs.

Local NGOs and Civil Society

At Millicom, we have extensively deepened our relations and interactions with civil society at a global, regional, and perhaps most importantly, local level. During 2018, we collaborated with various digital rights organizations in situations where we worked to counter threats to the principles of freedom of expression and privacy. We continue to deepen relations with digital rights organizations in our markets (such as TEDIC in Paraguay, Karisma in Colombia and Fundación Acceso in Costa Rica), seeing tremendous value in this multi-stakeholder approach where civil society and the private sector can work together to react to legislative or regulatory proposals which have implications for human rights. We believe it is important for both the private sector and civil society to collaborate and draw on the expertise of one another to put forward the most appropriate feedback to proposals by governments.

Often, we find that the motivation for government requests or action is driven by a legitimate public security concern, and that feedback and suggestions of best practices from other countries can help provide the safeguards needed to ensure rights-respecting solutions.

International financial institutions

Millicom continues to call for further safeguards by international financial institutions and the development aid community to protect freedom of expression. Any financial support from these agencies for the promotion of the Information and Communications Technology (ICT) sector should be accompanied by a clear set of criteria for the protection of freedom of expression and privacy.

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 mobile and fixed line voice and data, cable television, Mobile Financial Services (MFS) and business-to-business (B2B) solutions, in three South American countries. During 2018, Millicom invested a combined total of US$954 million in the South and Central America regions to further develop our mobile and fixed communications networks. Both investments guarantee better bandwidths and quality of internet experience and allow more services and innovation to be built on top of this access.

We hold the top market position in B2C Mobile, B2C Home and MFS in Paraguay, while we are generally either the largest or the second or third largest provider across services in Colombia and Bolivia. We are an important contributor to our markets, in terms of investment, taxes[8] and as a provider of employment and services (see Table 3 and our recently launched socio-economic report)[9].

Table 2
South America (Bolivia, Colombia and Paraguay)

B2C Mobile customers '000	Homes connected[10] '000	MFS customers '000
14,714	2,469	1,943

Table 3

Country	Customers '000	Workforce[11]	Population[12] '000
Bolivia	3,465	2,961	11,050
Colombia	8,291	4,406	49,070
Paraguay	2,958	4,999	6,811

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 on the GNI website.[13]

In Bolivia, the use of interception is restricted to exceptional circumstances (such as human-trafficking) in which we would receive court orders to activate lines. This technique has been extended to drug-trafficking related investigations as per legislation enacted during 2017. That said, the discussion around the implementation of interception techniques is ongoing with the authorities. Concerns over the security environment in the country ahead of upcoming elections has fueled debate over further monitoring and control mechanisms for communications services, as detailed in the 'Major Events' chapter of this report.

The procedures in Colombia mandate us to provide direct access for the authorities to our mobile network. There are regular audits to ensure we do not gain information about interception taking place, and strong sanctions (fines) are in place should we be found to do so. As a result, we do not possess information about 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 and for these lines we receive judicial orders which we review and assess, and open 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, the authorities mandate that we provide direct access to our mobile network. However, the procedures allow us to view the judicial order that is required for the authorities to initiate the interception and we are aware when interception occurs. We have the possibility to file a complaint before the Supreme Court of Justice should we deem that the order or interception does not follow the requirements defined in law.

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

[8] We report income taxes paid in our Annual Report, page 130
[9] https://www.millicom.com/media-center/features/millicoms-economic-footprint/
[10] Total Number of Households with an active service
[11] Workforce accounts for employees directly employed by Millicom
[12] Populations statistics as per World Bank (2017)
[13] https://globalnetworkinitiative.org/policy-issues/legal-frameworks/

Requests from law enforcement in 2018

As can be seen in Table 5, there has been a slight increase in the level of requests we have received from law enforcement authorities across our markets in South America in the past year. That said, the numbers are consistent when analyzing the last few years. There is a notable increase in the number of interception (i.e. live or real-time call surveillance) requests this year, which is the result of the full implementation of a direct access system in one country after technical changes from the prior year. There is also a sizeable increase in the amount of MFS requests we are receiving as this business grows and becomes more popular in our markets.

A number of our 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 issue of direct access is one which is attracting increased attention. The UN Special Rapporteur for Freedom of Expression has recently started a research piece in this area and the GNI has also focused on the issue as a policy priority.

It is worth repeating that the actual written request any operation receives counts as one request in the data tables. It should also be noted that one request may ask for information on several individuals or several devices.

Table 4

	Authorities who 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 and the Information and Financial Research Unit	Attorney-General's office, public prosecutors, judges
Paraguay	National Anti-Drug Secretariat (SENAD), National Secretary for Intelligence (SINAI) and Homeland Secretariat	Public Prosecutor's Office, Criminal Courts

Table 5

South America	Interception	MFS	Metadata	Metadata requests per customer
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%

The requests are therefore not 'equal' in magnitude. The great majority of the requests received are in the category of customer metadata. Most of these, in turn, are requests to confirm the identity behind specific phone numbers. Some requests may ask for information of more than one customer's mobile phone records (calls to and from, cell tower location) during a specified time-period or around a specific area.

The number of requests that our local operations receive also depend on how many customers we have and our market position. In South America, the percentage of metadata requests received per customer is 0.154% (which is nearly identical to last year's figure).

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 mobile and fixed line voice and data, cable television, Mobile Financial Services (MFS) and business-to-business (B2B) solutions.

During 2018, Millicom invested a combined total of US$954 million in the South and Central America regions to further develop our mobile and fixed communications networks. Both investments guarantee better bandwidths and quality of internet experience and allow more services and innovation to be built on top of this access.

We hold the top market position for many services across the region and we serve as an important contributor to our markets, in terms of investment, taxes[14] and as a provider of employment and services.

In addition to the four countries we are reporting on (Costa Rica, El Salvador, Guatemala and Honduras), we also have a small but growing business in Nicaragua. We had only catered to enterprise clients in Nicaragua until this year when we also began offering cable TV and DTH services. We have also, in December 2018, completed a transaction in Panama, becoming the 80 percent shareholders in the leading cable provider in the country.[15] While we are already reporting on a 'Major Event' linked to Nicaragua, moving forward we plan to include both Panama and Nicaragua in this particular section of our reporting also. From the beginning of our involvement in these operations we have been training our staff on our key policies and guidelines in the areas of freedom of expression and privacy.

Table 6

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

B2C Mobile customers '000	Homes connected[16] '000	MFS customers '000
17,705	1,186	1,943

Table 7

Country	Customers '000	Workforce[17]	Population[18] '000
Costa Rica	N/A[19]	586	4,906
El Salvador	2,500	598	6,378
Guatemala	10,708	3,012	16,910
Honduras	4,497	1,070	9,265

Legal frameworks

Due to challenging security environments, with high levels of organized crime and drug trafficking- related violence, governments in Central America have some of the most developed laws and technical surveillance requirements in place. In Costa Rica, where we operate fixed networks only, the number of requests are significantly lower than in other Central American markets.

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 have visibility on how often or for what periods of time interception takes place. In the case of 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, 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 these requests, review them and provide the authorities with the information requested.

In El Salvador and Honduras, special laws exist mandating telecommunications operators to block signals in and out of prisons. Similar laws had also been in place in Guatemala previously (see section 9 for a more extensive overview of prison signal blocking in the region).

As is the case in all our markets, we are not compensated at cost for the resources we need to put or have in place for assessing and processing requests from law enforcement. In the case of Central America, given the challenging security situation in numerous countries, these resources are extensive and must be available to respond to requests at all times.

[14] We report income taxes paid in our Annual report, page 130

[15] On February 20, 2019, Millicom announced it has entered into agreements with Telefónica S.A. and certain of its affiliates (Telefónica), to acquire the entire share capital of Telefónica Móviles Panamá, S.A., Telefónica de Costa Rica TC, S.A. (and its wholly owned subsidiary, Telefónica Gestión de Infraestructura y Sistemas de Costa Rica, S.A.) and Telefonía Celular de Nicaragua, S.A. (together, Telefonica CAM) for a combined enterprise value of US$1,650 million (the Transaction) payable in cash. The Transaction is subject to regulatory approvals in each market, expected during H2 2019.

[16] Total Number of Households with an active service

[17] Workforce accounts for employees directly employed by Millicom

[18] Populations statistics as per World Bank (2017)

[19] Millicom does not presently have mobile operations in Costa Rica, only B2C Home and B2B services, in which it is the market leader.

Requests from law enforcement in 2018

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 epidemic of violence afflicting these countries. Surveillance and customer data requests underpin law enforcement authorities' efforts to combat these serious challenges of organized crime. The differences in the sizes of populations between our Central American markets versus our South American markets can make direct comparisons from one region to the other difficult and previous notes made about requests not being 'equal' in magnitude further complicates such attempts.

As can be seen in Table 9, metadata requests have remained relatively static while interception and MFS requests have increased significantly. The fact remains that certain requests may be "bulk" requests for a large number of metadata records, which can often skew the numbers. Efforts to combat crime and corruption in one particular country continue to drive a large proportion of these requests and they remain the primary reason behind increases in requests. It is worth noting also that as the innovative MFS business segment grows, it is becoming an increasingly popular service (particularly in Central America where remittances are tremendously important to local economies) and with this increase in use comes increased attention from the authorities.

Table 8

	Authorities who 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

Table 9

Central America	Interception	MFS	Metadata	Metadata requests per customer
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. Africa

Overview

Millicom has had operations in Africa for nearly 25 years. Today, we provide Mobile, MFS and B2B solutions. During 2018, Millicom invested a total of US$40.5 million in the region (which now accounts for only 5% of Millicom's overall revenues) to modernize and expand the geographical coverage of our mobile networks.

In 2015, in Tanzania, Millicom acquired the operator, Zanzibar Telecom (Zantel), and in 2016, Millicom sold its operations in the Democratic Republic of Congo (DRC) to Orange. During 2017, Millicom decided to merge its operations in Ghana with those of (Bharti) Airtel. In the same year, Millicom also agreed to the sale of its Senegalese and Rwandan units. In line with these transactions, this year we are reporting on requests in Chad and Tanzania only. This makes comparison to previous years difficult due to the various acquisitions, mergers and divestments across the Africa region in recent years. We are the market leader in Chad, while we are in second position in Tanzania. We are an important contributor to our markets, in terms of investment, taxes and as a provider of employment and services.

Table 10

Africa (Chad and Tanzania)

	B2C Mobile customers '000	MFS customers '000
	15,911	6,863

Table 11

Country	B2C Mobile customers '000	Workforce	Population[20] '000
Chad	3,283	262	14,900
Tigo Tanzania	11,616	402	57,310
Zantel Tanzania[21]	1,012	164	N/A

Legal frameworks

Significant challenges exist with regards to the overall clarity of laws, legal oversight and separation of powers when it comes to legal surveillance frameworks across the Africa region. This has also been highlighted by research into legal frameworks and their application in the region by civil society organizations.[22]

In our African markets, there is generally a lack of clear laws and processes on who can make requests for surveillance, customer data or service suspensions, as well as how and in what circumstances those requests may be made. Legal frameworks are still developing across the region. This, coupled with challenges with rule of law and processes being followed, can make determination of the legality of requests received challenging.

Laws related to emergency and national security powers of the authorities are often broad. In essence this means that in emergency situations (which are themselves not clearly defined) the authorities are often within their powers to ask for significant actions from us, such as complete or partial shutdowns of services for any length of time. When national security powers are cited as reasons for such requests, strong sanctions for non-compliance typically will apply.

In Chad, a law was enacted in 2015 to establish an Electronic Security and Certification Agency to oversee any interference to communications networks, including interception. This body was recently created and is currently in the process of establishing itself in order to perform its mandate.

In Tanzania, we are mandated by law to provide the telecommunications regulator an updated list of customer information on a regular basis. In some operations, the same regulators operate a traffic monitoring system, which monitors network-use information (i.e., numbers of calls, minutes and transactions) for tax auditing purposes. In Tanzania, an additional monitoring system has been implemented to ensure that operators are billing correctly for services offered.

[20] Populations statistics as per World Bank (2017)

[21] Zantel is a brand which operates on mainland Tanzania and the island of Zanzibar. We are required to report our subscribers separately from our Tigo brand from a regulatory perspective.

[22] https://cipesa.org/2018/10/state-of-internet-freedom-in-africa-2018-report-focuses-on-privacy-and-data-protection/ https://paradigmhq.org/download/digital-rights-in-africa-report-2018/

Requests from law enforcement in 2018

The level of requests we receive from law enforcement authorities across our markets in Africa has remained relatively steady, with a slight increase in the number of metadata requests over the past few years. It should be noted that direct comparison with numbers from previous years is difficult due to divestment from certain assets (i.e., the DRC, Rwanda and Senegal), the merging of our operations in Ghana with Bharti Airtel and the acquisition of other assets such as Zantel.

The slight increase in the numbers shown in Table 13 can be attributed mainly to security and anti-corruption efforts in the region. As can be seen from the table above, there has been a gradual decrease in the number of MFS-related requests, which can be attributed to the divesture and deconsolidation of Millicom's operations in Africa.

Table 12

	Authorities who can request interception of metadata	**Authorities that can issue orders for interception**
Chad	Prosecuting Attorney, National Security Agency	Judge
Tanzania	Police officer with the written consent from Attorney General, Tanzania Intelligence and Security Service	President, Courts

Table 13

Africa	Interception	MFS	Metadata	Metadata requests per customer
2018	0	228	8,930	0.056 %
2017	0	251	7,705	0.036 %
2016	5	326	6,827	0.028 %
2015	5	354	5,326	0.018 %

8. Case Study

Last year, we decided to provide more specific details about the types and sources of requests received in one unnamed country. This year, we are providing the same detail, for the same country, allowing for a year-on-year data comparison.

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

Types of requests relating to metadata received in-country

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

Source of requests relating to metadata received in-country

Requests come from a range of actors. The Attorney General's Office, the National Police force and the country's judiciary continue to be behind most requests. These requests arrive with prior authorization from a relevant court or judge and are assessed for validity by our local legal team who accept or refuse the request accordingly.

Table 14

Customer metadata requests

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

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

* Note that all these numbers refer to a request that has been previously authorized by a court or judge.

9. Major Events in 2018

We call demands that fall outside of the three types of law enforcement assistance requests covered in previous sections 'Major Events'. All local operations are required to escalate these events to global management and take a number of steps in order to minimize the effect of such events on our services and on our customers' rights to freedom of expression and privacy. The events described in this section are those that were reported to global headquarters in 2018.

Deciding whether to challenge 'Major Events' is rarely simple given they have a legal basis, albeit these events frequently stem from broad national security related powers.

We define 'Major Events' to include: requests for shut down of specific base station sites, geographical areas or 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[23], denial of access for specific individuals, significant changes relating to surveillance techniques or operational processes (how local surveillance laws are implemented in practice), 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.

In 2018, we had a total of 20 events falling into the definition of 'Major Events'. This is an increase on the total reported in 2017 (14), and similar to figures we reported in 2015 (20) and 2016 (18). A large majority of the events were in Africa (14), with two in South America, and four in Central America. The events are broken down by type in Table 16. In 2018, anti-corruption efforts and security concerns are driving the uptick in 'Major Events' activity, while we have noted numerous irregular demands in the Africa region in particular.

As with law enforcement requests, there are no accepted or standardized definitions across the ICT sector for different types of 'Major Events' or how they should be accounted for.

In Millicom's case, we count number of actual requests that have been made directly to us, or events that have consequences or implications our services and the rights of our customers.

We count the event regardless of whether our engagement was successful in stopping it from happening or not. One request may include a shutdown of several different services, or request to shut down parts of the network in several different geographical areas. If we have been demanded to extend a previous shutdown, we count this as a new request.

In practice this means that, for example, in the case of a request for the shutdown of cell towers around prisons in Central America, we count one request per country instead of the number of prisons or cell towers that have been shut down. 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 'Major Event'. For example, this year, we are not reporting any 'Major Events' in this area as signal blocking continued during 2018 in much the same manner as it existed at the beginning of the year. Although we are not reporting ongoing signal blocking in prisons (or new blocking measures which do not impact our business directly) as a 'Major Event', we continue to consider this a major issue and will continue to provide details on its implications and the work we are doing to mitigate risks and threats to freedom of expression.

We have clear guidelines for our subsidiaries on what to do when faced with 'Major Events', in addition to escalating the information to the global team for assistance. When describing some of the events below, we are sometimes unable to describe the engagement we undertake to reduce the impact of these events to our customers' privacy or freedom of expression. We have, however, shared such information in different multi-stakeholder forums, some of which are described in section 4 on engagement.

Table 16

Type of major event

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

[23] With the exception of blocking of 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 operation and local management if sanctions defined by law are applied. Sanctions do not limit themselves to fines, but can in some cases also include imprisonment or removal of a license to operate communications networks. These types of requests often happen during a particularly volatile time of civil unrest, which means we must also consider the safety of our entire staff as well as potential retaliation from the general public against our company and our visible assets, such as shops and base station sites.

In 2018, as has been extensively covered in the media[24], there were several government-mandated disruptions to internet access and different social media across the Africa region. In Millicom's markets, there is an ongoing social media block in Chad. We also received numerous base shutdown requests during 2018 in Chad, as the country's security forces continue to fight terrorist threats in multiple regions of the country.

Although we have not received any shutdown orders in Tanzania, we have received specific content takedown requests. In Tanzania, we have seen an increase in the number of 'Major Events' from previous years. The underlying factors are less about national security and more often about attempts by the government to fight corruption and fraud by improving its own audit systems and processes. We are encouraging the relevant authorities to further develop legislation and regulation in this regard so as to improve protections for the freedom of expression and privacy of citizens.

Meanwhile, in Nicaragua, as has been reported in the press[25] we were required to move a TV Channel from the main channel line-up. In this case, the impact was very limited given our cable TV services offering has only been made available as of 2018 and our current customer base is still very small. That said, Nicaragua is a developing business for us and we are encouraged to see how seriously our staff has taken adherence to our internal guidelines, raising this instance immediately without fail for our consideration and decision-making.

Informing customers of shutdowns

In our emerging markets, mobile services are still to a large extent 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 when they are informed of new promotions, products or other issues of relevance. This means we can carry messages to our customers through our sales force, even when services are affected.

In the event of government-mandated service disruption, we always do our best to make it clear to our customers that we are dealing with a situation beyond our control. It is our experience that in most cases our customers are conscious of 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 cell phones that have been smuggled into the premises. Guatemala also enacted similar laws in 2014, but the relevant legislation was overturned in the Supreme Court in 2015. During 2018, Costa Rica's new government also introduced new signal blocking measures but these do not currently affect our service offering in the country. That said, we were involved in the monitoring and advocacy work performed by organizations such as the GSMA and ASIET in relation to the same.

In Central America, prisons are often located in central urban areas, which means the removal of antennae, shutting down of base station towers, and installation of 'jammers' can affect the mobile service of populations living in the vicinity of the correctional facilities, and may disrupt every day activity, such as the use of ATMs. Sanctions for non-compliance with these lawful orders include substantial fines and even the possible revocation of licenses.

We continue to actively engage with the authorities and industry peers, focusing on finding alternative solutions that would address the issue in a way that does not affect the population living in the vicinity of prisons. These include everything from new network coverage designs around prisons to third party solutions that work similarly to jammers to block signals in specific physical areas, to relocation of prisons outside of densely populated areas.

It should also be noted that Millicom is undergoing assessment on prison signal blocking in the Central America region, having been requested to provide this as a case study as part of the GNI Assessment process during 2018.

El Salvador

Due to the increase in extortions in El Salvador, an Anti-Extortion Law was approved in April 2015 under which any telecommunications signal inside prisons is prohibited. This legislation established daily fines of up to US$900,000 for non-compliance by a telecommunications operator.

Furthermore, if five fines were to be given within a single year, the license could be revoked.

As violence in the country hit a peak in March 2016, the National Congress approved a Law on Special Measures on April 1, 2016, which allowed the government to take specific drastic

[24] https://qz.com/africa/1524405/zimbabwe-protest-internet-shut-down-military-deployed-5-dead/
https://qz.com/africa/1513023/drc-shuts-down-internet-sms-ahead-of-election-results/
[25] https://confidencial.com.ni/ortegas-assault-on-independent-tv-channel-100-noticias/

measures related to at least seven prisons, if the signal were not blocked by the operators. These measures were revised and extended for an additional year in April 2017 before being approved on a permanent basis during 2018. The Legislative Assembly's Security Commission decided to reform the "Penitentiary Law" to make signal blocking a permanent rather than temporary mechanism.[26]

Because of this legislation, and at the government's request, operators have had to shut down their base station towers, not only near the prisons, but also in surrounding areas, leaving a part of the population in these areas without service. We have since taken measures to narrow and focus the scope of the blocking, to help mitigate freedom of expression 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 relating to national security efforts.

Telecommunications operators in the country continue to work jointly with the government to reduce and minimize the impact to service of customers near the prisons.

Honduras

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

The sanction for non-compliance is approximately US$420,000 for the first instance, while the second is approximately US$840,000, and the third results in termination of the license.

In 2014, several antennas were turned off to comply with the law, which meant that some users in large cities were left without service given that most prisons are located in populated areas. Operators are yet to find a blocking solution which limits the effects on the population outside of prison while circumventing the guards' ability to turn off the jammers.

In 2016, we had to extend signal blocking to three additional prisons and improve the effectiveness of the previously installed jammers. The Honduran telecommunications regulator, CONATEL, sent a written notification to announce the start of a sanctioning process after running tests at one of the prisons, where they had detected a signal permitting successful outgoing calls. In January 2017, both Tigo and the country's other large operator, Claro, were served with sanctions for outgoing calls. We are currently disputing this sanction in the courts.

Proposals for significant changes in operational procedures or local laws

In instances of proposals for changes in law enforcement procedures, we are often strictly prohibited by local laws to disclose details of proposed changes, as these relate 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.

There have been several developments around local legal frameworks and operational procedures in both of our regions.

Whenever laws are developed with an open and consultative process, we proactively engage with the authorities. The most common feedback we give to legislators is for establishment of judicial oversight, promotion of proportionate and necessary measures, and the importance to be as narrow, clear and detailed as possible regarding which authorities can make requests under the law, and what the requirements are in terms of response from us. We often find that legislators struggle with understanding the role and limitations of different players in the ICT ecosystem and, as a result, assign requirements to telecommunications companies that can only be carried out by providers of specific services.

We also disagree that telecommunications operators should bear the cost of implementation of technical and operational measures for interception, as is frequently proposed by governments. In our view, as such requirements are typically very costly and, moreover, in order to encourage the proportionate use of such powers, the cost should not be borne solely by mobile operators.

Bolivia

As the country approaches elections in 2019, there have been several noteworthy proposals put forward by the legislature. Citing a relevant provision from the 'Convención Americana sobre Derechos Humanos' President Morales is running for re-election, despite previously losing a referendum on his right to do so, which in turn has been met with some protests.This environment has created security concerns for the government and police forces, who have responded with legislation attempting to quell such concerns.

The government has attempted to propose a 'law against lies' which seeks to penalize and sanction promoters of misinformation. The proposal, however, is at a very early stage and has not progressed much after significant controversy over how it would be implemented. Another pending bill is one proposed by legislators via the police forces, who are seeking to counter crimes being carried out via the use of telecommunications. The bill, in its current form, could have a negative impact on privacy and FoE rights. Therefore, proactive engagement with the authorities is ongoing in an effort to find the right balance in meeting security concerns and protecting user rights. We remain attentive to any further threats that may emerge in the build up to elections in October.

[26] https://www.elsalvador.com/noticias/nacional/499058/bloqueo-a-senal-de-celulares-en-carceles-seria-permanente/

El Salvador

The Minister of the Interior and ruling party deputies presented a bill in October 2018 seeking to regulate content in cinema, TV, open signal and cable, radio and online advertisements. The proponents of the bill sought to address "mental health" and "promote a culture of peace, especially among younger people". However, the bill received heavy criticism from a number of sectors (and other political parties) who cited violations of the principles of FoE and has not progressed to date.

Honduras

In February 2018, the ruling party in Honduras introduced a bill aimed at combating hatred and discrimination online. The bill has already been discussed several times and is expected to be called for a final debate at any time. The bill, modeled on Germany's Netz DG law, requires any service or website that includes user-generated content to process complaints and remove "hate speech" or discriminatory content within 24 hours. Should online intermediaries fail to do so, their services could be fined or blocked. The bill also creates a national cybersecurity committee to receive reports and relay them to websites and companies, and to develop policy strategies on issues ranging from cybercrime to hate speech and fake news. We have been involved in advocacy efforts related to this bill via the local business chamber COHEP and also with our peers in the GNI.

Guatemala

A similar bill was presented in Guatemala's Congress, that targets "terrorist acts" and seeks to sanction (with penalties including jail-time) participants in "cyber-terrorism". One would be classified as such if they "instill alarm in the population on matters related to the Government." Initiative Law 5239 also contemplates the creation of a Communication Network "integrated by security, immigration and customs authorities, which allows optimizing control procedures without affecting the flow of trade".

The broad definition and diffuse limits cited in the bill have raised concerns among journalists and activists, who fear that it will be used to persecute and silence dissidents online. The Chamber of Journalists of Guatemala rejected the initiative, arguing that article 22 on cyberterrorism is a "veiled and brazen pretension to restrict the exercise of freedom of thought issuance". The bill is awaiting a second and third reading for approval but it has received strong criticism and other major political developments have taken precedence for now.

Other events

In Chad, the government continues its military efforts against Boko Haram. This group remains highly active around the Lake Chad region, with several terrorist incidents occurring in the past few years. The government is also engaged in military operations to the north of the country. This security context has led to a particularly tense and difficult environment where the local authorities are under intense pressure to uphold public safety. Strict laws on telecommunications operators' obligations, in relation to collaboration with the security forces in matters related to national security, can make it difficult to challenge requests and engage on issues related to the protection of freedom of expression and privacy rights. We have received a number of requests over of the past year and while we have tried to be as transparent as possible in this report, we remain restricted in terms of how much we can disclose on each event.

The same holds true for a number of 'Major Events' witnessed in Tanzania during 2018. As previously mentioned, the government's anti-fraud and anti-corruption efforts have resulted in an at times challenging environment with regards to requests. Local staff are often expressly prohibited from disclosing the nature or content of requests and our respect for local staff safety restricts how much detail we can give in this regard. That said, we remain engaged with civil society partners on the issues and, when possible, encourage authorities to strive to adhere to international standards when applying local law.

10. Trends and priorities for 2019

Trends in our operating environment

In 2018, as previously indicated, the number of 'Major Events' in our markets increased from the numbers we had registered in the previous period. The main underlying factor for this rise were numerous shutdown events in the Africa region, due to ongoing security issues in Chad. Anti-corruption efforts by the Tanzanian government also underpinned an increased number of extraordinary requests in this country. We expect both these trends to continue (and potentially increase in magnitude) into 2019. We will continue our work with authorities in both countries to improve and educate around the need for transparency, accountability and proportionate action.

Increased demands and some 'Major Events' in 2018 can be directly related to increased electoral activity in Millicom's Latin American markets. This was a busy electoral year in the region (there were elections in Costa Rica, El Salvador, Colombia, and Paraguay) and 2019 will also see several important elections take place (Bolivia, El Salvador, Guatemala, and Panama). With this in mind, we are prepared for the possibility that 'Major Events' could occur in any of these markets during 2019.

A trend highlighted in our previous reports—new proposals for laws relating to surveillance and cyber security—continued in 2018. This is a continuing trend as governments seek to understand how new technologies can help them in their national security efforts. Unfortunately, we often 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 (governments included) working on joint solutions, is the most effective way to understand and satisfy the demands and wishes of a representative share of the populace.

As ever, political and security related events or threats in our markets naturally impact developments related to privacy and freedom of expression. An increase in the number of 'Major Events' recorded this year for the Central American region can be directly related to such issues, with organized crime and gang violence a major focus for the authorities. Civil unrest due to electoral issues and corruption concerns also contributed significantly to the number of 'Major Events' recorded in the wider Latin America region.

Prison shutdowns will remain a significant challenge in the Central America region. Although we had no 'Major Events' recorded for this issue during 2018, it should be noted that the implementation of prison signal blocking measures in Costa Rica (where we are not currently affected as we do not yet have mobile operations) was a setback for industry advocacy efforts. We continue to work closely with organizations such as the GSMA, ASIET and COMTELCA to hold educational workshops on these issues with government representatives in the region.

An ongoing political crisis in Nicaragua resulted in the first-ever major event recorded in this country during 2018. As we continue to build out our business and meet our commitment to invest in bringing digital services to the Nicaraguan people, we remain alert to any extraordinary demands by the authorities. Our commitment to invest in the country must go hand-in-hand with our strong commitment to human rights while, in parallel, we must also comply with the law.

As mentioned, the number of shutdowns in Millicom markets in 2018 increased from the previous year. We hope to double our efforts with civil society and others to leverage the significant work carried out in recent years in drawing international attention to these issues. We have discussed this topic and shared best practices on several occasions with our industry peers. We have also successfully proposed that this topic be a policy focus area for the GNI and we remain encouraged by the potential of this group to address the issue with governments. Millicom supported the GNI in its work to produce a one-page guide for policy makers 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

It is prudent to remind those who read our transparency reports that most requests we receive outside of the established legal process often seem to stem from a lack of comprehensive understanding of the laws by certain law enforcement officials. Equally, the lack of capacity and capability (resources and knowledge) of local law enforcement in understanding the ICT ecosystem and/or having access to the latest cyber-investigation methods, often leads 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 of these are requests relating to content that we do not hold, such as that from social media services such as YouTube, WhatsApp or Facebook. Such data is held outside of the requesting jurisdiction, and complex mutual legal assistance treaties make it very difficult for local law enforcement agencies in country to promptly retrieve it.

At a local level, we meet with law enforcement agencies regarding disproportionate or overreaching requests or proposals. We do this in order to explain to and 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 such as independent oversight, narrow and focused orders for legitimate purposes only, strict time limits, and the ability to verify that the correct authorized individual(s) is carrying out the request.

Advocating for clear laws

As we consistently maintain in our transparency reports, clear laws and processes are crucial tools for telecommunications companies when it comes to respecting the privacy and freedom of expression of our customers. We operate local subsidiaries which are bound by local laws—perfect or not—and we do not have the option of selecting the laws with which we will comply. As a result, advocating for clearer laws—that respect international conventions and narrowly define who, how and in what circumstances law enforcement requests can be made—is crucial to protect privacy and free expression, even when it may take time to achieve the desired end result. We consider this a core instrument to promote proportionate use of such powers. Assessment of the legality of requests would be simplified, to the benefit of both privacy and freedom of expression rights of citizens. Clear laws would also bring efficiency to law enforcement processes, which in turn would help us to challenge requests should the law not be followed.

We continue to welcome additional technical assistance, from the international community to developing countries, that includes human rights considerations both in the area of cyber-investigations, as well as in designing transparent and clear laws around surveillance so as to ensure they incorporate international human rights law.

Priorities for 2019

We aim to continue our engagement efforts with all stakeholder groups around issues of freedom of expression and privacy, in particular network shutdowns and direct access. In addition, we will further promote related internal guidance by continuously monitoring the effectiveness of our existing guidelines and procedures in relation to law enforcement assistance. We recently rolled out new guidance in this regard at a local level, with in-person training sessions at regional summits. We take compliance with our internal procedures very seriously and have previously sanctioned employees for not following our guidelines and controls. This has been a natural evolution of our maturity process, where we now have a robust system and set of controls in place, following our initial implementation of this framework in 2015.

As it relates to external advocacy, we plan to 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 call for the need for human rights based technical support for legislators and law enforcement in our regions. Most importantly, perhaps, we will continue direct dialogue with relevant government agencies whenever possible.

We look forward to continuing to build on our recent membership of the GNI to jointly address challenges shared by this multi- stakeholder group. We are currently undergoing GNI's assessment process, and we welcome the opportunity to be assessed in this manner against the GNI principles.

Advocating and helping to define clear, transparent and effective surveillance laws with appropriate safeguards in place is an area we will continue to focus on going forward, as we continue to work with the GNI on the sensitive issue of direct access. Furthermore, as stated in the 'Major Events' section, a recent trend of countries revising their surveillance- and interception-related legislation is certain to continue. Having a clearer definition of what 'good' surveillance laws look like is a key way to support our operations as they strive to engage positively with the authorities on this topic.

Finally, we have now launched a comprehensive privacy policy framework which includes GDPR type standards. The policy is currently held on our website and we are working to build an online portal where users will be able to consult all our privacy-related policies and commitments, with relevant Q+A material and interactive tools.