MILLICOM
THE DIGITAL LIFESTYLE

Law Enforcement Disclosure Report

Millicom Law Enforcement Disclosure Report 2017

What's inside this report...

1. Introduction

This is Millicom's third Law Enforcement Disclosure (LED) report, covering the year 2017. It serves to provide information about the extent and context of our interaction with law enforcement agencies and governments relating to issues that affect the privacy or freedom of expression of our customers in Latin America and Africa.

Since the advent of WikiLeaks and the Edward Snowden information leaks, there has been ever increasing scrutiny in the public domain on the topics of privacy and freedom of expression in the digital age. Indeed, ongoing dialogue with our stakeholders informs us that these topics are among the most material corporate responsibility issues for stakeholders. However, telecommunications network providers are often caught in between the laws that are designed to protect citizens from the threat of terrorism and other crime, and those that are designed to protect the rights to privacy and freedom of expression.

As technology rapidly evolves, Millicom and other telecommunications network providers are part of a major shift in traffic from traditional voice and SMS services to new-age data services, in line with the demands of a hyper-connected world. At the same time, legislators and law enforcement agencies are struggling to keep pace with how to adapt to the implications that this shift in communications traffic is having on traditional and established methods and practices for requests for information related to criminal investigations. This fast changing landscape means that the need for multi-stakeholder engagement on such issues is greater than ever before.

In March 2017 Millicom, together with six other telecommunications companies, announced its membership of the Global Network Initiative (GNI). This organization, which now has over 50 members, brings together technology companies, ethical investors, academics and human rights organizations to 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. Building on the public commitment made by Millicom in 2013, as a founding member of the Telecommunications Industry Dialogue, to use any leverage we may have to minimize human rights implications of the demands we receive from governments, joining the GNI was a natural 'next step' for Millicom. We have made considerable progress over the past few years engaging with stakeholders around these complex issues and putting in place policies and processes that help us minimize negative impacts to freedom of expression and privacy. By becoming a member of the GNI, Millicom now has a platform on which to build further leverage by virtue of new relationships with other organizations which approach these issues from different perspectives but share the same ultimate goal. It is our firm belief that positive outcomes for human rights will only come from collaboration based on appreciation of the full spectrum of considerations and realities – something that can only be achieved when all concerned stakeholder groups, including governments, come together.

At Millicom, our customers' trust in us to respect their privacy and freedom of expression is of paramount importance for our business. At the same time, 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 freedom of expression. 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.

In this report, we aim to demonstrate our ongoing commitment and progress, how our operations impact human rights, and how we can work independently and with others to minimize potential negative impacts.

When we make decisions about government demands on our local operations, we consider not only the human rights of our customers, but also our legal obligations, any other potential impacts on the communities where we operate, any potential adverse consequences to the safety of our thousands of employees and partners who work with us to provide services in our markets, and any potential impacts to our operating licenses or the physical assets on the ground – radio towers and transmitters, cables, shops and offices. Millicom and its customers rely on these assets to receive uninterrupted access to communications and Internet services in the first place.

All of these aforementioned considerations impact the way in which we respond to demands from law enforcement agencies, and are fundamental aspects to consider in the discussion around our company's responsibility to protect freedom of expression and privacy.

Luxembourg, February 2018

Rachel Samrén
Executive Vice President
Chief External Affairs Officer

Salvador Escalón
Executive Vice President
General Counsel

At Millicom, our customers' trust in us to respect their privacy and freedom of expression is of paramount importance for our business. At the same time, 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.

2. Reporting at Millicom

Millicom is a leading provider of cable and mobile services dedicated to emerging markets. We operate under the Tigo brand in eight countries across Latin America and three in Africa. 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. Our mission is to provide the fastest, most secure digital highway so we become the first choice for customers in all our markets.

Millicom's two key motivations for publishing its LED report for 2017 remain the same as those which existed when we published our first LED report: (1) to respond to stakeholders who have asked us to be more transparent about how we deal with government requests, and (2) to advance the understanding of the contexts in which telecommunications companies receive demands from governments and the considerations influencing decisions in relation to these situations.

As an operator focused solely on emerging markets, we continue to 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, and 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) in an effort to provide more granular and detailed information about law enforcement requests. We also continuously study and implement lessons learned from our industry peers and civil society resources, predominantly through our association with the Global Network Initiative (GNI).[1] This year, we have included a section with a case study on one anonymized country to show the different types and sources linked to law enforcement assistance requests.

We hope that the third 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 amount of law enforcement requests we receive and, more importantly in our opinion, we describe the overall context and trends in the demands we receive. Context is important in specific and more significant cases – what we call 'major events'[2] – as it highlights some very practical challenges we encounter in our interactions with law enforcement authorities.

In this report, we also describe several 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 which 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.

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 forbidden by law from disclosing details of the requests we receive. In some specific 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.

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 we may try to challenge their approach. Doing so would most certainly affect our ability to engage in the future, and could even 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, we describe our engagement in more broad terms in this report rather than in relation to specific events.

We are not disclosing the numbers of government requests by country as some of our peers have done. The reasons for this are multiple. Disclosure in certain countries is legally forbidden. Only in Tanzania does the law explicitly state we are allowed to publish aggregate numbers of requests we receive. In the remaining countries, the law is either not clear as to whether we are allowed to publish the numbers of requests we receive, or it explicitly prohibits publication.

We have conducted considerable internal risk analysis and debate about publishing country-specific numbers. We operate in some countries where publicly disclosing such numbers may put the safety of our employees at risk. This is not necessarily a risk from government but rather 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 business 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, while we have this year added a specific country case study detailing the different types and sources of requests.

1 In previous editions we have reported our progress based on the Telecommunications Industry Dialogue (TID) principles. Since we recently joined the Global Network Initiative (GNI) we will no longer be reporting against the TID principles. Instead, from next year onwards, we will report against the GNI principles, following our first assessment process by the GNI.

2 Major events can include clearly politically motivated requests for: 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 also include information about the different types of communications services we provide in each country as well as numbers of customers and our market position – these all affect the numbers of requests we receive and should be taken into account when trying to determine the extent of government activities.

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[3] 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 continues to be no agreed or standardized definitions or ways to classify law enforcement requests across the Information, Communications and Technology (ICT) industry. Standardizing definitions is challenging given the multiple different jurisdictions and business models in our wider sector. At Millicom, we classify requests we receive into three distinct categories: requests for interception; customer metadata; and customer financial data (relating 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. All other types of requests, which fall outside of the definitions below, we report as 'major events'. We do not report on content take-down requests specifically as these are rare in our markets, with the exception of legally mandated removal of access to child sexual abuse content in Colombia. Any other content take-downs are accounted for under major events.

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.

How we obtain the material we report

The information on number of law enforcement demands we receive is reported to us by legal departments of each of our local subsidiaries. As prescribed in our 'Global Guidelines on Law Enforcement Assistance', these legal departments are in charge of receiving and reviewing all demands for their legality before they are executed. They log each demand by date, type (see table 1), and requesting authority. This information is recorded in dedicated tools or entered manually to templates provided by the Millicom Group. When requests are legally justified, these same teams provide the requested information to the authorities.

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

The Global Corporate Responsibility team collates and consolidates all of this information. The 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.

Major events information is collected throughout the year and a log is kept of these events by the Global Corporate Responsibility team. We are confident that if not all, at least the great majority of major events are now escalated to the Group, to our cross-functional Law Enforcement Disclosure Committee, comprising of senior staff from the External Affairs, Legal, Security, and Compliance functions.

This is the second 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 162 - 163 (limited assurance report).

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[4].

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

3. Our internal policies, guidelines and governance

Human rights impact and risk

Millicom recognized at an early stage the need to engage proactively on privacy and freedom of expression, to understand human rights risk relating 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 Group guidelines, adding controls and improving readiness of global and local teams to handle any major events situations and the reputational issues they pose. Initial focus has been on improving local processes by providing support to local management and the teams who manage law enforcement relationships.

In 2017, the first year of our membership in the GNI, we carried out a 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.[5] As part of this risk assessment, we have contracted external expert support to help 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 relating to specific situations. We nevertheless wish to formalize this assessment and broaden our analysis by interacting with external stakeholder groups to create a dynamic tool which we will update and consult on a regular basis.

Board and management committees – governance and oversight of human rights

All corporate responsibility activities in Millicom are overseen by our Board of Directors (BoD) as well as our Executive Committee (EC). The Board receives regular updates on corporate responsibility topics with Millicom's CEO, EVP Chief External Affairs Officer, and EVP General Counsel being permanent guests at these briefings. Millicom's EVP Chief External Affairs Officer reports to the EC on these topics on a monthly basis, and Millicom's VP Corporate Responsibility is responsible for the ongoing management of human rights issues in the company.

Millicom's BoD is being periodically updated on human rights issues and has directed management to continue its strong proactive approach and to deepen relationships with civil society on a country level. In 2016 and 2017, the BoD received an updated human rights risk assessment relating to privacy and freedom of expression. In 2018, we will deliver a fresh in-depth report on Millicom's risk exposure on these issues, as well as a detailed overview of all our human rights related work. Going forward, we will institutionalize this detailed update to the BoD on a yearly basis to ensure the highest levels of the company's management are kept abreast of our work in these areas and can provide their feedback on the same.

Back in January 2014, when Millicom began its escalation process efforts, 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 VP Corporate Responsibility, EVP General Counsel, EVP Chief Ethics and Compliance Officer, Chief Information Security Officer, VP Legal Latam and Chief Privacy Officer, and Regulatory Affairs Directors. The Group members prepare and jointly approve policies and processes, review our 'Major Events Guidelines' and arising risks, and approve Millicom's reporting and engagement relating to privacy and freedom of expression. The LED Committee met twice in 2017 to review risks and actions related to freedom of expression and privacy. 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 2017, the first year of our membership in the GNI, we carried out a 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.

In 2017, we continued our work on a global privacy policy framework. Millicom's EC approved broad privacy principles and commitments for the company and guidelines, 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 framework development is followed by a steering committee consisting of four of Millicom's EC members (EVP Chief External Affairs Officer, EVP Ethics and Compliance

5 https://maplecroft.com/

Officer, EVP Chief Technology and Information Officer and EVP General Counsel) and our privacy policy is expected to be finalized early in 2018. We will also be rolling out this framework internally and externally during 2018, including the completion of Millicom's privacy commitments and guiding principles. All of the 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 are included in the updated Millicom Code of Conduct, which was approved in 2017.

In addition, Millicom has signed up and made a commitment to implement the Principles on Freedom of Expression and Privacy for the Telecommunications sector as defined by the Telecommunications Industry Dialogue (TID). The TID Principles called on us to publicly report on how we are implementing and 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 on these commitments following our first assessment process with the GNI which is expected to occur during Q4 of 2018.

Millicom's Group Guideline for Law Enforcement Assistance Requests (LEA Guideline) was finalized and approved by the LIP Committee (now LED Committee) in Q1 2015. It is reviewed yearly. The LEA guideline clearly outlines 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.

Our internal control process assesses how well our subsidiaries apply and comply with different global policies and controls. Two controls relating to the implementation of the LEA Guideline were added in the Millicom Internal Control Manual in 2015. The first checks 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 subsidiaries 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 subsidiaries making substantial improvements in the maturity level of their controls for the LEA guidelines. In 2017, all operations achieved one of the two highest maturity levels, meaning that 100% of our subsidiaries now have an acceptable level of controls implemented at a local level.

'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 provides practical suggestions on how to engage with the authorities so as to limit the remit and/or timeframe of any 'major event'. Due to the sensitive nature of this document, it is not publicly available but we have presented its contents in meetings with the TID and the GNI.

In 2017, we began an assessment of how we can better streamline communication of these internal policies, guidelines and controls to our local staff. We are conducting an external benchmarking of how this is done across the industry and we aim to create one authoritative, streamlined document in order to make sure our internal resources are easily understood and 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, and came into effect July 1, 2015.

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. New employees must complete the IS training within ninety (90) days of job commencement, and IS awareness materials are distributed to all employees at least annually.

4. Our engagement

Millicom continues to work proactively with a wide range of actors in order to mitigate against negative 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 as full members, having spent 2016 as observer members. We have also engaged with a number of international organizations and took part in various events, contributing to the ongoing debate around freedom of expression and privacy, as it evolves in the context of a rapidly changing technological landscape.

In response to a recommendation by our Board of Directors, at the end of 2015 we signed a three-year donation agreement with the international human rights organization Civil Rights Defenders to increase bilateral sharing of information on situations in our markets and to create connections with local human rights defenders.

Concurrently, we engage directly with governments and other in-country stakeholders on the topic as much as possible. We seek to enhance governments' understanding of our obligations also 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 face these challenges 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 on these issues internally on a continuous basis.

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.

We are encouraged by the work of the Swedish Export Credit Corporation (SEK/EKN) in this area, and we hope this will serve as an example for further international financial institutions to learn from these best practices.

In 2017, upon consultation by SEK/EKN, Millicom and its peers in the Telecommunications Industry Dialogue (TID) provided input on a paper being drafted in conjunction with the Institute for Human Rights and Business.

Telecommunications Industry Dialogue (TID)

Millicom was a founding member of the TID on Freedom of Expression and Privacy, a joint industry group working since 2011 on principles, tools and joint advocacy to meet the challenges to privacy and freedom of expression. Millicom held a Board seat in the former TID and Chaired the initiative in 2014-2015. Other members included Vodafone, Orange, Telefónica, AT&T, Nokia, TeliaCompany, and Telenor. Millicom strongly advocated for TID to merge with the Global Network Initiative (GNI), and in the beginning of 2016, we and six other members of the TID joined the GNI as observer members for a one-year period. That period ended in March 2017, when Millicom and other members of the TID formally joined the GNI. The final TID Annual Report was issued in 2017, with a particular highlight being the Industry Dialogue's interaction with Privacy International (PI) to provide its joint position on direct access.

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 GNI implementation guidelines that will be expanded to address a wider range of ICT sector companies. We have also participated in a number of sessions and pieces of work related to Internet shutdowns and their negative effects on economies and social activities.

Millicom welcomes the continued collaboration and further leverage it has secured as a full member, 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. In March 2017, Millicom met with UN SR David Kaye at Rightscon, where Kaye previewed his June report to the UN Human Rights Council. Kaye's report addressed the roles played by private actors engaged in the provision of Internet and telecommunications access. Millicom had helped provide input on this report at previous consultations in Geneva as well as a 'brainstorming session' with the SR held by Article 19 in London in July 2016. Millicom had also participated at a further expert consultation session held by the University of Connecticut in October, which helped contribute to Kaye's report. This year, Millicom continued to provide formal written feedback to the SR on his upcoming work, in collaboration with the GNI.

UNICEF

Millicom and its local subsidiaries sustain regular contact and engagement with UNICEF. We take part in regular calls as part of a working group with other industry representatives from across the ICT sector. As part of this group we have been providing input and feedback to UNICEF on a new Toolkit on Privacy / Freedom of Expression. 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. This year, Millicom released the MOCRIA (Mobile Operators Child Rights Impact Assessment) tool that we developed together with UNICEF, providing our operations with the right framework and targets to improve our practices around children. The MOCRIA is available to all operators and has been widely acclaimed. In a report published by UNICEF highlighting our work on Child Rights, Andrew Mawson, Chief of Child Rights and Business for UNICEF, stated:

"I commend Millicom for taking leadership on child rights, for being transparent on its findings, learnings and areas for improvement. Above all, I commend them for recognizing that the job is never done and that this is a continuous work in progress. I encourage other companies to think carefully about what child rights means for them and hope that this report serves as an example for how to undertake or broaden their own child rights journey[6]."

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 2017, we collaborated with various digital rights organizations in situations where we worked to counter threats to the principles of freedom of expression and privacy. Specifically, we have deepened relations with digital rights organizations TEDIC (Paraguay) and Karisma (Colombia) at a local level. We see tremendous value in this multi-stakeholder approach where civil society and the private sector can work in tandem 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 one another's expertise in order to put forward the most appropriate solutions as 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 often provide the safeguards needed to ensure rights-respecting solutions.

We seek to enhance governments' understanding of our obligations also outside of their countries, while repeatedly highlighting the risks from disproportionate government action, especially to their reputation and foreign investment possibilities.

6 http://www.millicom.com/media-room/features/unicef-commends-millicom/

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 2017, Millicom invested a total of US$907 million in the South and Central America regions combined 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 the second or third biggest provider across services in Colombia and Bolivia. We are an important contributor to our markets, in terms of investment, taxes[7] and as a provider of employment and services (see table 3).

Table 2
South America (Bolivia, Colombia and Paraguay)

B2C Mobile customers '000	Homes connected[8] '000	MFS customers '000
14,322	2,232	1,498

Table 3

Country	B2C Mobile customers '000	Workforce[9]	Population '000
Bolivia	3,303	2,996	11,100
Colombia	7,851	4,730	49,200
Paraguay	3,167	4,689	6,852

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 by the TID.[10]

In Bolivia, the use of interception is restricted to exceptional circumstances 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.

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. Hence, we have no 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 defined at maximum six months in the law.

In Paraguay, as in Colombia, the authorities mandate us to 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.

Requests from law enforcement in 2017

As can be seen in table 5, there has been a gradual and slight decrease in the level of requests we have received from law enforcement authorities across our markets in South America over the past few years. Some of our countries in the region have direct access, which means we are not notified of all instances in which customer communication is being intercepted.

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.

7 We report income taxes paid in our Annual Report, page 116
8 Total Number of Households with an active service
9 Workforce accounts for employees directly employed by Millicom
10 http://www.telecomindustrydialogue.org/resources/colombia/

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
2017	38	21	21,492	0.150%
2016	111	73	22,521	0.103%
2015	184	104	24,447	0.115%

There has been a gradual and slight decrease in the level of requests we have received from law enforcement authorities across our markets in South America over the past few years. Some of our countries in the region have direct access, which means we are not notified of all instances in which customer communication is being intercepted.

The requests are therefore not 'equal' in magnitude. The great majority of the requests we receive 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 depends on how many customers we have and our market position. In South America, the percentage of metadata requests received per customer is 0.15%. The reason why this figure has increased while the number of requests have decreased, is linked to a significant reduction in the number of mobile customers registered in Colombia following a large-scale clean-up of our customer database.

6. Central America

Overview

Millicom has operated in the Central America region for over 25 years. We provide a wide spectrum of services in five different markets, including mobile and fixed line voice and data, cable television, mobile financial services (MFS) and business-to-business (B2B) solutions. During 2017, Millicom invested a total of US$907 million in the South and Central America regions combined 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 a number of services across the region and we serve as an important contributor to our markets, in terms of investment, taxes[11] and as a provider of employment and services.

In addition to these four countries, we also have a small B2B business in Nicaragua, for the moment only catering to enterprise clients. We recently secured cable TV and DTH services licenses in the country also.

Table 6

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

B2C Mobile customers '000	Homes connected '000	MFS customers '000
17,589	1,070	2,153

Table 7

Country	B2C Mobile customers '000	Workforce[12]	Population '000
Costa Rica	N/A[13]	609	4,929
El Salvador	2,796	627	6,400
Guatemala	10,169	2,647	17,077
Honduras	4,625	1,112	9,340

Legal frameworks

A challenging security environment with high levels of organized crime and drug trafficking-related violence, means that governments in Central America have some of the most developed laws and technical requirements in place for surveillance. 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 for the authorities to our networks. However, the laws in both countries specify the authorities that can request interception and the actual interception orders can only be granted by the courts (see table 8). However, as access is direct 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 period of time specified.

Law enforcement authorities across our markets in Central America continue their efforts to tackle crime and violence in the region, with murder rates in El Salvador and Honduras some of the highest in the world outside of war zones.

11 We report income taxes paid in our Annual report, page 116
12 Workforce accounts for employees directly employed by Millicom
13 Millicom does not have mobile operations in Costa Rica, providing only B2C Home and B2B services, in which it is the market leader.

For customer metadata, judicial orders from the same courts are required in all four 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 been in place in Guatemala previously also and there is a possibility that they may return following recent incidents drawing political attention to the matter (see section 9 for a more extensive overview of prison signal blocking in the region).

As is the case in all of 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 a number of countries, these resources are extensive and must be available to respond to requests at all times.

Requests from law enforcement in 2017

Law enforcement authorities across our markets in Central America continue their efforts to tackle crime and violence in the region, with murder rates in El Salvador and Honduras some of the highest in the world outside of war zones. 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 America markets versus our South America 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.

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
2017	933	160	10,848	0.060 %
2016	816	194	16,758	0.099 %
2015	0	158	8,653	0.052 %

Although much fluctuation can be seen in Table 9, with metadata requests significantly declining in 2017, the fact remains that these requests can often be "bulk" requests for a large number of metadata records. Efforts to combat crime and corruption in one particular country continue to drive a large proportion of these requests, and the reduction in metadata requests from 2016 to 2017 can be rather misleading. We instead see an increasing level of demands in terms of overall requests. The level of interception requests increased slightly from 2016 to 2017, while we were not able to collect the number of interception requests in 2015 (and hence reported zero). MFS related requests continue to be a small proportion of the overall total of requests.

7. Africa

Overview

Millicom has had operations in Africa for close to 25 years. Today, we provide Mobile, MFS and B2B solutions. During 2017, Millicom invested a total of US$81 million in the region to modernize and expand the geographical coverage of our mobile networks.

In 2016, Millicom sold its operations in the Democratic Republic of Congo (DRC) to Orange, and in 2015, in Tanzania, Millicom acquired the operator, Zanzibar Telecom (Zantel). During 2017, Millicom decided to merge its operations in Ghana with those of (Bharti) Airtel. 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, Rwanda 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 generally in second position in our other African markets. 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, Rwanda, and Tanzania)

B2C Mobile customers '000	MFS customers '000
17,467	7,961

Table 11

Country	B2C Mobile customers '000	Workforce	Population '000
Chad	3,320	270	15,123
Rwanda	2,836	144	12,353
Tigo Tanzania	10,431	403	58,188
Zantel Tanzania[14]	881	153	N/A

Legal frameworks

Significant challenges exist with regards to overall clarity of laws, legal oversight and separation of powers when it comes to laws around surveillance across the Africa region. This has also been highlighted by research into legal frameworks and their application in the region by civil society organizations.[15]

Only one of our African operations could be said to have clear laws and processes on who is allowed to 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 in the process of developing across the region. This, coupled with challenges with rule of law and existing laws and processes being followed, makes determination of the legality of requests we receive challenging.

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.

14 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.
15 CIPESA: *State of internet freedom in Africa* http://cipesa.org/?wpfb_dl=225; PIN: http://pinigeria.org/paradigm-initiative-releases-2017-digital-rights-in-africa-report/

In all of our African operations, the laws relating to emergency and national security powers of the authorities are 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 extreme actions from us, such as complete or partial shutdowns of services for any period of time. When national security powers are cited as reasons for such requests, strong sanctions for non-compliance will apply.

While some judicial oversight exists for requests in most of our African operations, in two countries the President can also order interception. 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, although this agency is yet to be established.

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

Table 12

	Authorities who can request interception or metadata	**Authorities that can issue orders for interception**
Chad	Prosecuting Attorney, National Security Agency	Judge[16]
Rwanda	Rwanda Defense Force, the Rwanda National Police, and the National Intelligence and Security Service	National Prosecutor
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
2017	0	251	7,705	0.036 %
2016	5	326	6,827	0.028 %
2015	5	354	5,326	0.018 %

Requests from law enforcement in 2017

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 and Senegal) and the acquisition of other assets such as Zantel.

The increase to the numbers shown in Table 13 can be attributed to security efforts in the region, with particular concerns in one of our operations driving the increase in metadata requests. As can be seen from the table above, there has been a gradual decrease in the number of MFS related requests.

16 This only applies to metadata requests

8. Case Study

In line with our efforts to continuously improve our transparency standards we have decided this year to provide more specific details about the types and sources of requests received in one unnamed country. We made the decision to anonymize this data in order to respect local disclosure requirements and protect our local staff. We hope that 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 during 2017.

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 were behind the majority of 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)
Biographical details (owner of phone number)	58.05 %
Call and event registers	34.79 %
Coverage data and antenna locations	3.20 %
Contract copies or originals	3.08 %
Details related to potential acts of fraud	3.05 %
IP Address location	0.12 %
Requests to redirect emergency service calls	0.07 %
PUK Code (code to unlock SIM card)	0.05 %
Account information i.e. payment details	0.04 %
Blackberry PIN	0.02 %

Table 15
Source of Customer Metadata requests

Country	Percentage of total (January – Dec 2017)
Attorney General's Office	46.86 %
National Police Force	33.91 %
Judges	10.76 %
Other Entities	7.67 %
General Comptroller of Accounts	0.15 %
National Army	0.49 %
National Tax Authority	0.12 %
Lawyers*	0.03 %

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

9. Major Events in 2017

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 2017.

Decisions to challenge major events that are direct demands to us are rarely simple. Given the broad powers that exist in many countries for national security situations, we would be seen to be breaking local law by challenging requests that rely on a legal basis. The sweeping nature of those laws can be questioned, but it can also be questioned whether private businesses should engage in civil disobedience and, if so, who would determine in which cases this would be appropriate.

Not all major events are demands from the authorities. 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[17], 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.

Table 16
Type of major event

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

In 2017, we had a total of 14 events falling into the definition of major events. This is a slight decrease on previous figures we reported in 2015 (20) and 2016 (18). Seven of the events were in Africa, five in South America, and two in Central America. The events are broken down by type in Table 16. This year, there has been a substantial increase in the amount of events reported as 'Other'. This demonstrates how current legislative frameworks need to mature and evolve in order to keep pace with a fast-changing technology ecosystem which is resulting in an increasing amount of irregular demands outside of normal, defined and established government powers.

As with law enforcement requests, there are no accepted or standardized definitions 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 involved our services. 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 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 reporting Honduras as a single major event in terms of prison signal blocking, due to attempts to broaden the scope of the relevant legislation, but not in El Salvador, where signal blocking continued during 2017 in much the same manner as it existed at the beginning of the year. Although we are not reporting ongoing signal blocking in prisons as major events, we continue to consider this a major issue and will continue to provide details on its implications and the work we are doing to try and 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 major 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.

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

9. Major Events in 2017 – continued

Shutdowns

When we receive requests for shutdowns or service restrictions, we must consider direct consequences for our operation or 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 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 2017, as has been extensively covered in the media,[18] there were several government-mandated disruptions to Internet access and different social media across the Africa region. In Millicom's markets, however, we did not receive any major network disruption requests. Instead, we received a more specific content takedown request related to betting websites in Tanzania.

When we receive requests for shutdowns or service restrictions, we must consider direct consequences for our operation or 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 license to operate communications networks.

Meanwhile, in one country in Latin America, we received a verbal request to be prepared for the takedown of a particular TV Channel in the midst of electoral turmoil, but the request was never followed up on or actioned. In this case, we reminded the authorities that we would require a written copy of this request pointing to the relevant legislation permitting this action.

Informing customers of shutdowns

In our emerging markets, services are predominantly 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 are able to carry messages to our customers through our sales force, even when services are affected.

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 aware 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. The issue remains under discussion, however, and similar debates have also been taking place regionally. In Guatemala specifically, the issue has been brought into the spotlight again recently after the murder of several Movistar (Telefónica) employees who were said to have refused to pay extortion fees to gangs.[19]

In Central America, prisons are often located in central urban areas, which means removal of antennae, shutting down of base station towers, and installation of 'jammers' have an effect on 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 law orders include substantial fines and even the 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 design 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.

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 given within one year, our license could be revoked.

A joint solution was informally agreed between operators and the telecommunications regulator, reducing signal strength in and near prisons. Violence in the country hit a peak in March 2016, however, and on April 1 2016, the National Congress approved a Law on Special Measures which allowed the government to take specific drastic measures in relation 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. The measures are due to be revised again in April 2018 and may be extended or revoked at this point. This will follow legislative elections in El Salvador a month earlier, which will likely have an impact on the decision.

18 See:
https://qz.com/1091516/cameroon-internet-shut-down-as-southern-cameroons-ambazonia-protests-grow-in-bamenda-buea/
https://www.nytimes.com/2017/02/10/world/africa/african-nations-increasingly-silence-internet-to-stem-protests.html

19 http://www.estrategiaynegocios.net/lasclavesdeldia/1125803-330/telef%C3%B3nica-habla-sobre-las-extorsiones-en-guatemala-es-terrorismo

Because of this legislation, and at the request from the government, the 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.

Immediately after the government enforced these extraordinary measures, we informed our customers about the shutdowns and their possible implications on our service, explaining that we are obligated to comply with the measures relating to national security efforts.

Currently all of the telecommunications operators in the country are working jointly with the government to try to find a joint technical solution to reduce or 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 implies termination of the license.

In 2014, several antennas were turned off to comply with the law, which meant that many users in large cities were left without service given that most prisons are located in populated areas. Although we have implemented several different solutions, we have yet to find a solution which circumvents the guards' ability to turn off the jammers or stop cellphones entering the facilities.

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 our Tigo and Claro were served with sanctions for outgoing calls. We are currently fighting this penalty in the courts.

We are also currently working together with the industry and the government to find a joint suitable technical solution that would neither require blocking wider telecommunications signals nor result in the imposition of sanctions for telecommunications companies.

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 processes 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 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 are allowed to make requests under the law, and what the requirements are in terms of response from us. We also often find that legislators struggle with understanding the role and limitations of different players in the ICT ecosystem and may hence 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 do not benefit mobile operators, and, moreover, in order to encourage the proportionate use of such powers, the cost should not be borne solely by mobile operators.

Honduras
In January 2017 the National Congress of Honduras attempted to fast-track a number of changes to its intelligence and surveillance laws. The proposals sought to extend signal blocking in prison to include satellite services, Wi-Fi, Bluetooth, and similar technologies, while making the telecommunications providers solely and financially responsible for blocking these signals. The proposals also attempted to broaden the government's surveillance powers and reduce judicial oversight. According to the proposed amendment, the moves were necessary to "remove operational obstacles" in current security activities.

When we were notified of the package of amendments we immediately engaged with local associations, industry peers and Congressmen in order to share our concerns and feedback on the measures. The proposals were delayed as a result of our initial engagement, with the government taking the time to consider potential changes. During this window of opportunity, we pursued further engagement with regional and global stakeholders such as the GNI, Human Rights Watch and Civil Rights Defenders. This collaborative effort contributed to the successful reversal of the majority of the proposals, with discussions around potential changes to signal blocking legislation still ongoing. The other amendments around the broadening of surveillance powers and lessening of judicial oversight were dropped by Congress following concerns and feedback received from civil society and the private sector.

9. Major Events in 2017 – continued

Tanzania
In January 2017, the government issued 'The Electronic and Postal Communications (Online Content) Regulations, 2017' which placed obligations on "online content providers" to remove "indecent content/ material" and "hate speech" within strict timeframes or face sanctions of at least US$2,200 and/or 12 months of jail. This type of legislation is similar in vein to Germany's recently passed Network Enforcement Act, which went into effect in October 2017. Under this law social media companies could face severe fines for failing to remove hate speech. Furthermore, Sections 4 (1) (a) and 7 (1) (a) provide for all bloggers to register with the local telecommunications regulator the TCRA, which applies to Tanzanians living outside the country also.

Bolivia
A new law was issued in Bolivia in March 2017, which provided for the interception of communications for cases of illegal trafficking of "Controlled Substances". This legislation, which permits direct access to our network for investigations related to drug trafficking, was passed in the country's legislature without the consultation of the industry. The implementing regulation was jointly discussed with the authorities however, allowing us to advocate for safeguards such as maintaining ultimate control over the technical operation of opening and closing the line for interception. There are also clear references to the fact that operators need to receive relevant judicial orders to comply with the authorities' requests in such cases. Our local operation consulted with the local authorities, including the telecommunications regulator (ATT) and the Vice Ministry of Telecommunications, in order to push for judicial oversight, which was included in the Supreme Decree regulating the law issued in December 2017. We have until December 2018 to install interception equipment and implement relevant operating procedures.

Paraguay
Paraguay's Congress passed legislation on Aug 21, 2017 which "Regulates the Activation of the Mobile Telephony Service". The provisions of this bill included obligations around digital finger print registrations for users, including the retroactive registration of our entire customer database within one year. Failure to register would have resulted in the obligation to cancel these telephone lines. Additionally, company representatives would have been personally liable for any violation of the regulation.

The proposal for forced collection of biometric data was a particular concern in Paraguay due to the lack of comprehensive data protection regulation in the country. The lack of clear regulation on data protection may have created space for multiple interpretations that could have harmed our users' rights. With these risks in mind, we undertook a multi-pronged stakeholder engagement strategy in order to secure a presidential veto on the bill. A local industry media campaign was launched and we collaborated with civil society and local NGOs to raise awareness of this issue. These actions successfully led to the Executive power issuing a veto which has since been confirmed by Congress meaning that the bill has been retracted and will not be made into law.

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. 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 push back on requests and engage on issues related to the protection of freedom of expression and privacy rights. We have received a number of extraordinary requests over of the past year but remain restricted in terms of how much we can publicly disclose on these matters. All incidents are related to the country's ongoing fight against terrorism. We must, however, comply with laws, recognize the security situation, and respect the safety of our local staff and assets as priorities above public disclosure in such circumstances.

In Millicom's markets in Latin America, there are a number of important elections upcoming during 2018. This meant that a number of political party primaries occurred in 2017. During one of these events, we received a legal request for information which concerned individuals we deemed to be political rivals to the incumbent political power. We deemed this to be a major event due to the suspected political motives behind the demand. However, the request was within the country's legal frameworks and was accompanied by relevant judicial authorization, therefore we were restricted in terms of being able to challenge this request and remain restricted in how much we can publicly disclose on this item. Elections in this country will take place during 2018, and any further disclosure on this issue may be deemed locally as political interference.

In Paraguay specifically, as has been recently covered extensively in the local media[20], we received a request for call records, some of which fell outside the stipulated six-month time period during which our systems are required by local regulation to preserve such details. We were able to find a solution whereby our engineers reconstructed these call records using our billing systems (which hold information for a period of one year). It has since been claimed by the case prosecutor that certain requests for information were falsified and illegitimate. The latter is being reviewed by the Paraguayan Government with our full cooperation.

20 http://www.ultimahora.com/una-telefonia-ya-no-cuenta-datos-completos-cruce-llamadas-n1128135.html

10. Trends and priorities for 2018

Trends in our operating environment

In 2017, the number of major events in our markets slightly decreased from the numbers we had registered in 2015 and 2016. That said, the challenges and reactive work around these events remain a high priority for Millicom. The difference in the numbers of major events between 2017 and previous years, may be attributed to a reduced amount of electoral activity in Millicom's markets in the Africa region during 2017. Indeed, there is a direct correlation here between this and the decrease in the amount of 'shutdowns' we experienced last year. Furthermore, the decision to not report ongoing prison signal blocking obligations as additional major events contributed to this reduction. A trend highlighted in our 2016 report – new proposals for laws relating to surveillance and cyber security – continued in 2017 also. This is likely to be a recurring trend as governments seek to understand how new technologies can help them in their national security efforts.

The number of shutdowns in Millicom markets in 2017 was reduced greatly from the previous year.

We hope to see a continuation of this trend, with civil society and private actors having carried out significant work in recent years to draw international attention to these issues.

As ever, political and security related events or threats in our markets naturally impact developments relating to privacy and freedom of expression. Although there was a reduction in the number of major events recorded this year for the Central American region in particular, organized crime and related gang violence continues to be a significant issue and the non-recording of ongoing prison shutdowns as major events does not suggest we no longer work on these issues or fail to consider them as a threat to freedom of expression. We continue to work closely with organizations such as GSMA, ASIET and COMTELCA to hold educational workshops on these issues with government representatives in the region. We are particularly conscious of a recent situation in Guatemala where several Movistar (Telefónica) employees were killed by gang members for supposedly refusing to pay extortion fees. This incident was believed to have been directed and ordered by incarcerated gang leaders via phone calls, meaning that signal blocking in Guatemalan prisons is a topical issue once again. We are currently collaborating as an industry with the government to propose solutions. Additionally, an electoral crisis in Honduras towards the end of 2017 perhaps spelled some warning signs for a tumultuous 2018 – a significant electoral year in Latin America, with elections not only in four of Millicom's markets (Costa Rica, El Salvador, Colombia, and Paraguay) but also in two of the region's biggest economies (Mexico and Brazil).

Meanwhile, we witnessed a decrease in the number of major events in Africa in 2017 but continue to monitor issues related to various countries' fights against terrorism and corruption.

As mentioned, the number of shutdowns in Millicom markets in 2017 was reduced greatly from the previous year. We hope to see a continuation of this trend, with civil society and private actors having carried out significant work in recent years to draw international attention to these issues.

Millicom supported the GNI in its work to produce a one-page guide for policy makers and government officials, in order to ensure they fully understand the consequences of network shutdowns. In 2017, however, complete or partial shutdowns took place in several other African countries where we do not operate, and we remain attentive to this regional trend. The #KeepItOn campaign by Access Now continues to play an important role in highlighting these events, by aggregating information about shutdowns and building awareness.[21] This is a topic we have also discussed on several occasions with our industry peers, sharing best practices. We are encouraged that, via our membership in the GNI, we are now able to discuss engagement strategies with Internet companies and civil society in order to further mitigate against and reduce these practices.

Capacity of local law enforcement

Many requests we receive outside of the established legal process appear to be the consequence of 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, lead to our operations receiving requests that we are unable to carry out or that are disproportionate to the issue the authorities are trying to solve.

A common example of requests we receive but are not able to carry out, are requests for content that we do not hold, e.g. from social media services such as 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.

21 https://www.accessnow.org/keepiton/

10. Trends and priorities for 2018 – continued

At a local level, we meet with law enforcement agencies in relation to disproportionate or overreaching requests or proposals, in order to explain and educate 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

Clear laws and processes are crucial tools for telecommunications companies to respect privacy and freedom of expression of our customers. We operate local subsidiaries which are bound by local laws – imperfect or not – and we do not have the option of selecting the laws with which we will comply. Hence, even when it may be the longer route, advocating for clearer laws – respecting international conventions and narrowly defining who, how and in what circumstances law enforcement requests can be made – is crucial to protect privacy and free expression.

Clear laws and processes are crucial tools for telecommunications companies to respect privacy and freedom of expression of our customers. We operate local subsidiaries which are bound by local laws – imperfect or not – and we do not have the option of selecting the laws with which we will comply.

This is a core instrument to promote proportionate use of such powers. Assessment of the legality of requests would be much simplified to benefit both privacy and freedom of expression of citizens, and also bring efficiency to law enforcement processes, with the existence of clear laws. Clear laws would also better help us to challenge requests when they are not following the law.

Overall, we would welcome more technical assistance that includes human rights considerations to developing countries from the international community both in the area of cyber-investigations, as well as in designing transparent and clear laws around surveillance.

Priorities for 2018

We aim to continue our engagement efforts with all stakeholder groups around issues of freedom of expression and privacy, including network shutdowns, and further promote related internal guidance. In terms of internal guidance specifically, we will be undertaking an overhaul of our existing guidelines and procedures in relation to law enforcement assistance. We will subsequently roll out this new guidance at a local level with in-person training sessions at regional summits. In terms of external advocacy, we plan to attend major civil society events in 2018, such as for example RightsCon, and we will continue to 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 due to undergo GNI's assessment process in the last quarter of 2018, and we welcome the opportunity to be assessed in this manner against the GNI principles. In previous LED reports we have self-reported against the Telecommunications Industry Dialogue's principles but going forward we will now be reporting in line with the GNI principles and assessment process.

Advocating and helping to define what is clear surveillance law is an area we will continue to focus on going forward, as we expect that the trend we have seen in recent years of countries revising their surveillance and interception related legislation will continue. Having a clearer definition of what clear surveillance law looks like is a key way to support our operations to engage positively with the authorities on this topic. The GNI has also published the TID's legal frameworks resource which includes a large majority of Millicom's markets.

Finally, we aim to launch a comprehensive privacy policy framework in 2018 which will include an online portal on Millicom's website where users will be able to consult all our privacy-related policies and commitments.

Designed by
FleishmanHillard Fishburn
www.fhflondon.co.uk

MILLICOM
THE DIGITAL LIFESTYLE

For further information please contact:
cr@millicom.com

millicom.com