Law Enforcement Disclosure Report 2016

MILLICOM
THE DIGITAL LIFESTYLE

Law Enforcement Disclosure Report 2016

Contents

1. Introduction

This is Millicom's second Law Enforcement Disclosure report, covering the year 2016. It seeks 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 when we operate telecommunications networks in thirteen countries in Latin America and Africa.

The topics of privacy and freedom of expression remain highly relevant for companies providing communications services. In the last year alone, several high-profile incidents have led to even more intense scrutiny in the public domain. One example was the Apple vs. FBI case, where the company refused a request from the intelligence authorities to build a 'backdoor' in its iPhone devices in order to assist with a suspected murder investigation. This incident highlighted the tension that can at times exist between law enforcement authorities, who have a duty to protect their citizens, and technology companies who have a responsibility to protect the privacy of their customers' communications.

Our customers' trust in us to respect their privacy is of paramount importance for our business success. This consideration for human rights obligations must also go hand-in-hand with our duty to respect local laws in the countries where we operate; laws which legally bind us to support governments in their legitimate duty of protecting public safety and security.

In this report we present how we manage the tension that can at times arise between these obligations. We aim to demonstrate our ongoing commitment and progress to understand how our operations impact human rights, and how we can work alone and with others to minimize potential negative impacts.

Millicom made a public commitment in 2013 to the Telecommunications Industry Dialogue Guiding Principles to use any leverage we may have to minimize human rights implications of the demands we receive from governments. We have made good progress since then in implementing processes to do so. However, some fundamental tensions remain. There are many considerations we must take into account by virtue of being very integrated in the countries where we operate. Many of the tensions would not exist if the customer data we hold resided in servers outside of the country and we were providing services remotely from outside of local jurisdictions.

When we make decisions about government demands on our local subsidiaries, we do not only consider the human rights of our customers or our legal obligations, but also 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 – all of which we and our customers rely on 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 company responsibility in protecting freedom of expression and privacy. They also take our company to the heart of some of the most complex issues facing governments and the world today, and are clearly not something one company like Millicom can or should attempt to solve alone. This year, Millicom became an observer member of the Global Network Initiative and continued to engage with a number of different stakeholder groups, directly as well as jointly with the Telecommunications Industry Dialogue. 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.

> “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.”

In 2017, Millicom will join GNI as a full member and we look forward to working with GNI members and further improving our processes and understanding of these issues to be a long-term, responsible and positive influence in the countries we work in.

Luxembourg, February 2017

Rachel Samrén
EVP Chief External Affairs Officer

Salvador Escalón
EVP and General Counsel

2. What we are reporting, not reporting and why

Millicom Group (Group) is a telecommunications and media company, providing mobile and fixed internet, cable and satellite TV services, and mobile financial services (MFS) to consumers and businesses in thirteen markets in Latin America and Africa.

Two reasons remain central to our motivations in publishing this 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.

We regularly seek to identify best practices in the area of transparency reporting on law enforcement assistance, and attempt to implement these norms into our own reporting framework. With that in mind, we have this year divided our reporting for Latin America into two regions (Central and South America) in an effort to provide more granular and detailed information about law enforcement requests. We have also studied and implemented lessons learned from civil society resources such as the Transparency Reporting Toolkit: Reporting Guide & Template produced by The Berkman Klein Center for Internet & Society at Harvard University in collaboration with the Open Technology Institute[1]. Namely, we have included a section detailing how we obtain our information for this report in order to provide more clarity to the reader.

We hope that the second 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, describe the overall context and trends in the demands we receive. Context is important not only in specific and more significant cases – the so called 'major events' – but also in highlighting 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.

In line with the commitments that we have made to implement the Telecommunications Industry Dialogue (TID) ten principles[2] we also disclose information about our internal policies, processes and controls which we have put in place to protect our customers' privacy when we handle law enforcement requests, and how we seek to minimise effects on our customers' freedom of expression and privacy in 'major events' situations. You can find a table at the end of this report outlining how we have implemented the TID ten principles overall.

What we are not reporting

Law enforcement demands are by definition sensitive in nature. In most 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 situation we may be explicitly told not to disclose any details of the request, and doing so could lead to severe penalties, including imprisonment of local senior 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 leverage and 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 from 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.

[1] https://cyber.harvard.edu/sites/cyber.harvard.edu/files/Transparency_Reporting_Guide_and_Template-Final.pdf
[2] http://www.telecomindustrydialogue.org/about/guiding-principles/

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. This is the case in three countries. 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 the disclosure of numbers might, in our risk/benefit assessment, lead to negative outcomes to 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. This year we are splitting Latin America into Central and South America, which offers more granularity for the numbers as compared to previous years.

This year we also include information about the different types of communications services we provide in each country, our market position, as well as numbers of customers as these all affect the numbers of requests we receive and should be taken into account when trying to determine the extent of government surveillance activities.

We are finalizing reports about the legal frameworks governing government surveillance powers together with the law firm Hogan Lovells to cover all of our operating markets which are not yet covered by the Telecommunications Industry Dialogue legal frameworks resource[3]. We expect these to be published under the Creative Commons license by the end of Q1 2017. For this reason, we are not outlining specific laws by country as these will be included in the up-coming reports 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 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 financial services we provide). Some of our peers in the TID report in similar categories (see Table 1 for more detailed definitions of the three 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 extremely 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 in the 'other' category.

> “This year we include information about the different types of communications services we provide in each country, our market position, as well as numbers of customers as these all affect the numbers of requests we receive and should be taken into account when trying to determine the extent of government surveillance activities.”

[3] http://www.telecomindustrydialogue.org/resources/country-legal-frameworks/

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 6), 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 also provide the requested information to the authorities.

Information of major events is reported according to an escalation mechanisms defined in Millicom’s “Major Events Guideline”. 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 MFS 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 all, or at least the great majority, of major events are now escalated to the Group to our cross-functional Lawful Interception Committee, comprising of senior managers from external affairs, legal, security, communications and compliance function; two years after the launch of our escalation process.

Table 1
Definitions for 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 Financial Services (MFS) related data	Information relating to the MFS services we provide, such as confirming an individual is a customer, transaction data and other account activity. These requests do not always only relate to financial crime.

This is the first year that all of the numerical information relating to law enforcement demands was externally audited within our corporate responsibility reporting assurance carried out by EY. This makes us confident on the quality of the data we report, even when in most countries data collection is still managed through manual processes.

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 these issues in general. Please contact CR@millicom.com or find our full contact details on our website.

3. South America

Overview

Millicom has operated communications networks in South America for over 25 years. We provide a wide spectrum of services including mobile, cable and fixed line, as well as mobile financial services and B2B solutions, in three South American countries. During 2016, Millicom invested a total of $961 million in the South and Central America regions combined to further develop our mobile and fixed communications networks and purchase further spectrum licenses. 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 mobile, cable and MFS in Paraguay, while we are generally the second or third biggest provider in Colombia and Bolivia. We are an important contributor to our markets, in terms of investment, taxes[4] and as a provider of employment and services (see table 2).

Legal frameworks

In Bolivia and Paraguay clear processes and requirements exist for judicial oversight over interception and customer metadata requests. In Colombia, much due 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[6].

In Bolivia, the use of interception is restricted to very exceptional circumstances in which we would receive court orders to activate lines.

Table 2

Customers in South American region by business unit

	Mobile customers '000	Cable customers '000	MFS customers '000
South America	14,476	2,066	1,454

Table 3

Customers, workforce and population in South America

Country	Mobile customers '000	Workforce[5]	Population[7] '000
Bolivia	3,076	2,718	11,700
Colombia	7,764	24,918	48,800
Paraguay	3,635	4,509	7,100

The procedures in Colombia mandate us to provide direct access to 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.

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.

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 Supreme Court of Justice should we deem that the order or interception does not to follow the requirements defined in law.

[4] We report income taxes paid by region in our Annual report 2016, page 23

[5] Workforce accounts for both employees directly employed by Millicom and outsourced workers.

[6] http://www.telecomindustrydialogue.org/resources/colombia/

[7] The source for all population data in this report is the International Monetary Fund (IMF), 2015.

Table 4
Competent authorities

	Authorities who can request interception or metadata	Authorities who 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 Secretary	Public Prosecutor's Office, Criminal Courts

> "There has been a decrease in the level of requests we have received from law enforcement authorities across our markets in South America in 2016 compared to 2015."

Requests from law enforcement in 2016

As can be seen in table 5, there has been a decrease in the level of requests we have received from law enforcement authorities across our markets in South America in 2016 compared to 2015. It is worth noting that some of our countries in the region also have direct access, which means we are not notified of all instances in which customer communication is being intercepted.

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

The requests are 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. We have included more detailed information from one country to illustrate the types of requests relating to metadata we receive (Table 6).

Table 5
Requests from law enforcement in South America

South America	Interception	MFS	Metadata	Metadata requests per customer
2016	111	73	22,521	0.103%
2015	184	104	24,447	0.115%

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 0.103%, which helps provide some context for comparisons against the figures we show for the Central America (0.099%) and Africa (0.028%) regions.

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 in South America during 2016.

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 by a relevant court or judge and are assessed for validity by our local legal team who accept or refuse the request accordingly.

Rejected requests

In countries that have systematically recorded the numbers of requests they reject, the number remains (similar to 2015) at around 3-4% of all requests. The most common reason for rejecting requests is that the authorities are not following due process and the requests lack the correct signatures and stamps, or on occasion are made by parties who, by law, are not allowed to make them or are made without the proper legal oversight.

Table 6

Breakdown of customer metadata requests by type

Type	Percentage of total (January – Sept 2016)
Biographical details (owner of phone number)	59.44
Call and event registers	29.21
Details related to potential acts of fraud	5.77
Contract copies or originals	4.09
IP Address location	0.78
Coverage data and antenna locations	0.43
Blackberry PIN	0.20
Requests to redirect emergency service calls	0.07
PUK Code (code to unlock SIM card)	0.01
Account information i.e. payment details	0.00

4. 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, cable and fixed line, as well as mobile financial services and B2B solutions. During 2016, Millicom invested a total of $961 million in Central and South America regions combined to further develop our mobile and fixed communications networks and purchase further spectrum licenses. 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[8] and as a provider of employment and services.

In addition to these four countries, we also have a small cable business in Nicaragua, for the moment only catering for enterprise clients.

Legal frameworks

Largely due to a challenging security environment of organized crime and drug trafficking related violence, governments in Central America have some of the most developed laws and technical requirements in place for surveillance of our markets.

In Costa Rica, where we operate fixed networks only, the number of requests are significantly lower than in other markets.

In Honduras and El Salvador, the law mandates direct access for the authorities to our networks. However, the laws in both countries specify authorities that can request interception and the actual interception orders can only be granted by the courts (see table 9). However, as access is direct we do not receive these orders nor have visibility to 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 interception can be applied to in addition to other requirements. In Guatemala, interception also takes place under judicial orders, which we receive and review, and open the line for the period of time specified.

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.

Table 7

Customers in Central American region by business unit

	Mobile customers '000	Cable customers '000	MFS customers '000
Central America	17,529	1,034	2,247

Table 8

Customers, workforce and population in Central America

Country	Mobile customers '000	Workforce[9]	Population '000
Costa Rica	N/A[10]	708	4,900
El Salvador	3,213	1,377	6,400
Guatemala	9,468	4,154	16,300
Honduras	4,848	2,385	8,600

[8] We report income taxes paid by region in our Annual report 2016, page 23.

[9] Workforce accounts for both employees directly employed by Millicom and outsourced workers.

[10] Millicom does not have mobile operations in Costa Rica, providing only cable and B2B services in which it is the market leader.

In El Salvador and Honduras special laws exist mandating telecommunications operators to block signals in and out of prisons. Similar laws were in place in Guatemala until this year (see section 6 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 2016

Comparatively to 2015, the level of requests we have received from law enforcement authorities across our markets in Central America has increased in line with a significant increase in efforts to tackle crime and violence in the region. Surveillance and customer data requests continue to underpin law enforcement authorities' efforts to combat serious challenges of organized crime in the region.

As can be seen in Table 10, metadata requests have nearly doubled, reflecting efforts in particular in one country to combat crime and corruption. The number of interception requests are not comparable to 2015, as 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 but continue to grow in line with the expansion of this business segment.

Table 9
Competent authorities

	Authorities who can request interception or metadata	Authorities who 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 10
Numbers of requests in Central America by category

Central America	Interception	MFS	Metadata	Metadata requests per customer
2016	816	194	16,758	0.099 %
2015	0	158	8,653	0.052 %

> Comparatively to 2015, the level of requests we have received from law enforcement authorities across our markets in Central America has increased in line with a significant increase in efforts to tackle crime and violence in the region."

5. Africa

Overview

Millicom has had operations in Africa for close to 25 years. Today, we provide mobile, mobile financial services and B2B solutions in five different markets. During 2016, Millicom invested a total of $160 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 Tanzania, Millicom acquired the operator, Zanzibar Telecom (Zantel). 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[11] and as a provider of employment and services.

Legal frameworks

Significant challenges exist with regards to overall clarity of laws, absence of legal oversight or separation of powers when it comes to laws around surveillance across the Africa region. This has also been highlighted by some recent research into legal frameworks and their application in the region by civil society organizations.[13]

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. As described in section 6 of this report, 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.

Table 11
Customers in Africa region by business unit

	Mobile customers '000	MFS customers '000
Africa	24,681	8,084

Table 12
Customers, workforce and population in Africa

Country	Mobile customers '000	Workforce	Population '000
Chad	3,132	447	11,900
Ghana	3,933	674	27,400
Rwanda	2,966	278	11,600
Senegal	3,646	321	15,100
Tigo Tanzania	10,743	1,056	50,600
Zantel Tanzania[12]	988	215	50,600

Interception powers have been defined in law in all of our operating markets in Africa, but standards-based lawful interception installations were not in place in any of our markets at the end of 2016.

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 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 type of judicial oversight exists in most of our African operations for requests, 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. This agency is yet to be established.

[11] We report income taxes paid by region in our Annual report 2016, page 23
[12] 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.
[13] CIPESA: State of internet freedom in Africa http://cipesa.org/?wpfb_dl=225; PIN: http://pinigeria.org/2016/wp-content/uploads/documents/research/Digital%20Rights%20In%20Africa%20Report%202016%20%28HR%29.pdf

In two of our markets, Ghana and Tanzania, we are mandated by law to provide the telecom 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 the network use information, i.e. numbers of calls, minutes and transactions – for tax auditing purposes (to tax our subsidiaries on these services).

Requests from law enforcement in 2016

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 from the previous year. It should be noted that the 2015 and 2016 numbers are not directly comparable as 2015 includes requests in the DRC, while 2016 exclude these but include requests made to Zantel.

The increase to the numbers shown in Table 14 is mostly 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 below, there has been a very slight decrease in the number of MFS related requests witnessed in 2016 compared to 2015, despite the business itself increasing in size.

> Legal frameworks are in the process of developing across the Africa 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."

Table 13
Competent authorities

	Authorities who can request interception or metadata	Authorities who can issue orders for interception
Chad	Prosecuting Attorney, National Security Agency	Judge[14]
Ghana	President, senior police officers with the written consent of Attorney General and Minister of Justice, National Communication Authority	President, courts
Rwanda	Rwanda Defense Force, the Rwanda National Police, and the National Intelligence and Security Service	National Prosecutor
Senegal	Prosecutor, judge, police officer, military authorities and the telecommunications ministry authorities	N/A
Tanzania	Police officer with the written consent from Attorney General, Tanzania Intelligence and Security Service	President, Courts

Table 14
Numbers of requests in Africa by category

Africa	Interception	MFS	Metadata	Metadata requests per customer
2016	5	326	6,827	0.028 %
2015	5	354	5,326	0.018 %

[14] This only applies to metadata requests

6. ‘Major Events’ in 2016

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. You will find more details on this process in section 8 of this report.

The events described in this section are those that were reported to global headquarters in 2016.

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[15], 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 2016, we had a total of 18 events falling into the definition of major events. This is similar to the figure we reported in 2015, which was 20. Eleven of the events were in Africa, four in Central America, and another three in South America. The events are broken down by type in Table 15.

As with law enforcement requests, there are no accepted 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 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.

Table 15
Major events in 2016 by type

Type of major event	2015	2016
Shutdown of services	8	8
Proposal for significant changes in local laws	3	5
Proposal for significant changes in technical or operational procedures	3	2
Disproportionate customer data or interception requests	2	1
Politically motivated messages	2	1
Other	2	1
Total	20	18

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.

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 in most cases 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 9 on engagement.

Shutdowns

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 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.

When we receive requests for shutdowns or service restrictions, we must consider direct consequences for our 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.

[15] With the exception of blocking of child sexual abuse content, which in 2016 took place only in Colombia.

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 last year. The issue remains under discussion, however, and similar debates are taking place in Costa Rica also.

In Central America, prisons are often located in central urban areas, which means removal of antennas, shutting down of base station towers, and installation of 'jammers' has 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 $750,000 for non-compliance by a telecommunications operator. Furthermore, if five fines are given within one year, our license could be revoked.

A joint solution was informally agreed between operators and the telecommunications regulator, reducing the signal strength and activating existing blockers. This did not work efficiently, however, due to sabotage of the blockers by prison staff (under direct pressure from the gangs).

Violence in the country hit a peak in March 2016, and on April 1 the National Congress approved a Law on Special Measures allowing the government to take specific drastic measures in relation to at least seven prisons, if the signal was not blocked by the operators.

Because of this legislation, and at the request from the government, the operators had to shut down their base station towers, not only near the prisons, but also in surrounding areas, leaving a large part of the population in these areas without a 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 telecom 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 September 2015, the National Congress of Honduras passed a law establishing an obligation for telecommunications operators to block any telecommunications signal reaching the country's prisons.

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

> “All telecom operators in El Salvador are continuing to work 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.”

In 2014, several antennas were turned off to comply with the law, which meant that many of our customers in large cities were left without service given that most prisons are located in populated areas. Although several different solutions have been implemented, we have not been able to find a solution that would circumvent the guards' ability to turn off 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.

We continue to work together with the industry and the government to find a joint suitable technical solution that would not require blocking wider telecommunications signals nor would result in the imposition of sanctions for telecommunications companies.

Shutdowns in Africa

In 2016, as has been extensively covered in the media,[16] there were several government-mandated disruptions to internet access and different social media. In our operations, the most extensive restriction took place in Chad during the election weekend in April, followed by a social media ban lasting several months. In March, the authorities ordered telecommunications providers to block access to Facebook, citing national security provisions of the law. The shutdown lasted 72 hours.

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.

Proposals for significant changes in operational procedures or local laws

In all instances of proposals for changes in law enforcement procedures, we were 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 of being 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 internet 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 also in order to encourage the proportionate use of such powers, the cost should not be borne solely by mobile operators.

Tanzania

In April 2015, Tanzania adopted a new Cybercrime Act 2015, which was immediately criticized by human rights groups, particularly

> “We 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 internet services.”

[16] See: https://qz.com/696552/more-african-countries-are-blocking-internet-access-during-elections/ https://rsf.org/en/news/media-obstructed-during-chads-presidential-election

relating to Article 16 which forbids "publication of false information". The government had agreed to carry out a review of the Act as a result, but to our knowledge this has not yet taken place. Instead, in 2016, the government has begun enforcing Article 16.

In 2016, the telecommunications regulator of Tanzania enacted Cybercrime Act Regulations outlining more clearly the legal obligations of service providers such as Tigo and Zantel with regards to the Cybercrime law. The regulation includes obligations to provide customer metadata information to competent authorities as well as data retention requirements for 12 months. These regulations also describe obligations for take-down of content that 'infringes on the rights of individuals'. There is, however, a recourse for providers such as Tigo and Zantel to challenge take-down requests on legal grounds. So far, we have not received any content take-down requests based on this new regulation.

Ghana
At the end of 2015, the Ghanaian government introduced a proposal for a new Interception of Postal Packets and Telecom Messages Bill. Tigo in Ghana has submitted extensive comments to the bill in 2016 jointly with the industry. The bill has also received feedback from civil society and opposition parties, who have criticized Parliament for a short consultation period. Due to the large amount of feedback on the proposal, as well as 2016 being an election year, the Bill was not voted on in Parliament in 2016.

Paraguay
In July 2016, the Paraguayan government introduced a law for mandatory parental controls to be provided by ISPs providing access to the internet for families with children. There are several open questions relating to how the law will be implemented, which may have important human rights implications and which we are following up, such as whether it would apply also to internet cafes and free public wifi spots, as well as who provides the filters.

Disproportionate requests
Costa Rica in 2016 introduced a new resolution that allows the Ministry of Treasury (in charge of taxes) to request the country's internet service providers to provide their entire customer data base to the Ministry - including name, ID number, address, service contracted and telephone number. The reason for the measure has been cited as controlling tax revenue and possible tax evasion.

Our local subsidiary appealed the resolution as disproportionate after we received the first request for our customers' information. The Ministry of Justice rejected our appeal, forcing us to comply with the request. We are still considering challenging the resolution in a higher court. As we finalize this report, discussion is under way with the Industry Chamber on the practical process of sending this information, focusing on the importance of keeping the information secure.

Politically motivated messages
There are cases where our services may be used for political purposes. At the end of December 2016, our customers in Paraguay received messages about the possible re-election of the sitting President, who is currently serving his last constitutional term. There was a strong reaction in the media and our Tigo subsidiary was accused of spreading political propaganda. The reality of the matter was that the message was sent by a client of a company to whom we have sold SMS advertising space and without our knowledge of the content. We are now examining arrangements highlighted by this case and the need to introduce new internal guidance for these types of services to avoid such events in the future.

> “In Costa Rica, our local subsidiary appealed the government request for our customers' information as disproportionate. The Ministry of Justice rejected our appeal, forcing us to comply with the request. We are still considering challenging the resolution in a higher court.”

7. Trends and priorities for 2017

Trends in our operating environment

In 2016, the number of major events remained at the same level as in 2015 in our markets. There was an increase in proposals for laws relating to surveillance and cyber security. This is a trend we expect to continue in 2017, as many governments are seeking to understand how new technologies can help them in their national security efforts.

Political and other events in our markets naturally impact developments relating to privacy and freedom of expression. In this respect, it has been another tumultuous year in many of our markets in 2016. As previously mentioned, organized crime and related gang violence continues to be a significant issue in Central America. A crack-down on corruption continued in Guatemala following the ousting of the president in 2015 and spilled over to Honduras, to an extent. Africa has experienced an increase in terrorist incidents. Chad continued to engage militarily against Boko Haram. Presidential elections were held in two of our markets in 2016: Chad and Ghana. A further two will take place in 2017 – in Rwanda and Honduras.

In our markets the number of shutdowns remained at the same level as the previous year and continue to be more common in Africa than Latin America. The trend we are seeing is to move towards more "surgical" shutdowns rather than wider shutdowns of the entire network, which would draw further international attention. Shutdowns are most frequently requested for basic SMS messaging services, or for popular social media services such as Facebook, Twitter, Viber and WhatsApp – rather than for the whole internet or base station sites in a specific geographic location. This year we also received a request for the first time for throttling of services, showing developing sophistication in applying restrictions to access.

Despite a strong declaration on freedom of expression and the internet against shutdowns by the UN special rapporteurs and signed by the African Commission on Human and Peoples' Rights, shutdowns appear to be increasing in the region. Complete or partial shutdowns took place in several other African countries where we do not operate, and this trend is likely to continue across Africa in 2017.

Concurrently, there has been a very positive trend of multi-stakeholder collaboration and strong statements against shutdowns – including the one we signed jointly with the TID and GNI[17]. We have been sharing our experiences of shutdowns in several forums also in 2016. Great work has been done on the economic impacts of shutdowns this year[18], and initiatives such as #KeepItOn campaign by Access Now[19] are aggregating information about shutdowns and building awareness. This is a topic we have discussed on several occasions with our peers in the TID, sharing best practices.

We hope that with our membership in the Global Network Initiative, we are able to discuss ways in which internet companies that are often the target of these shutdowns may join us in engagement on the ground with governments to stop these practices.

Capacity of local law enforcement

Many requests we receive outside of the due legal process appear to be the consequence of lack of comprehensive understanding of the laws themselves 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.

[17] https://www.globalnetworkinitiative.org/news/global-network-initiative-and-telecommunications-industry-dialogue-joint-statement-network-and

[18] See study by Brookings "Internet shutdowns cost countries $2.4 billion last year" https://www.brookings.edu/research/internet-shutdowns-cost-countries-2-4-billion-last-year/

[19] https://www.accessnow.org/keepiton/

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 who 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 - are crucial to protect privacy and free expression. 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. This is something we hope to also explore with the GNI.

Priorities for 2017

We will continue to engage with all stakeholder groups around the issue of shutdowns, and further promote related internal guidance. We are also keen to discuss these issues with members of the GNI to see how we can jointly address some of the challenges.

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 2015 and 2016 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. We will publish information on current legal frameworks of all of our markets with TID.

Finally, in external advocacy, we will continue to promote the need for further safeguards on human rights in international development aid and financial assistance as well as the need for human rights based technical support for legislators and law enforcement in our regions.

> 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 2015 and 2016 of countries revising their surveillance and interception related legislation will continue.”

8. 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: both to understand human rights risk relating to our operations and put in place processes to manage them.

We have taken several steps to minimize our risks where we can, introducing Group guidelines, adding controls, as well as 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.

We carry out an annual 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. For this country analysis we rely on VeriskMaplecroft's risk indices[20].

Our significant presence in our markets means we have a good understanding of the potential risk situations and risk levels relating to specific situations. We have, nevertheless, in 2016 begun work on a more formalized human rights impact assessment with external expert support. We expect to complete this work in early 2017, and the assessment becoming a dynamic analysis tool we 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 independent Board of Directors (BoD) as well as Millicom's Executive Committee (EC). In a change to 2015, instead of a separate committee, the whole Board now receives regular updates on corporate responsibility topics. Millicom's CEO, EVP Chief External Affairs Officer, and EVP General Counsel are 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 of Corporate Responsibility is responsible for the on-going management of human rights issues in the company.

In 2015, we provided Millicom's BoD a detailed report on Millicom's risk exposure in relation to privacy and freedom of expression and current mitigation measures. The BoD advised Millicom to continue its strong proactive approach and to deepen relationships with civil society on country level. In 2016, the BoD received an updated human rights risk assessment relating to privacy and freedom of expression.

In January 2014, to better coordinate risk management of the issue, Millicom established a cross-functional 'Lawful Interception Policy Committee' (LIP Committee) chaired by the VP Corporate Responsibility with as members: EVP Chief External Affairs Officer, VP Security, EVP General Counsel, Director of Communications, and Director of Compliance. The Group meets on a regular basis and its members prepare and jointly approve policies and processes, review 'major events' and arising risks, and approve Millicom's reporting and engagement relating to privacy and freedom of expression. The committee met three times in 2016.

In 2016, we began work on an aligned global privacy policy framework. Millicom's EC approved broad privacy principles for the company and guidelines and supporting decision guides 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 Officer, CTIO and EVP General Counsel) and is led by VP Associate General Counsel and VP Corporate Responsibility.

[20] https://maplecroft.com/

8. Our internal policies, guidelines and governance – continued

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 2015.

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). One of the TID Principles calls on us to publicly report on how we are implementing and putting the then principles into practice. This report is that public account (see section 10 for the full table).

Millicom Group Guideline for Law Enforcement Assistance Requests (LEA Guideline) was finalized and approved by the LIP 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.[21]

Our internal control process assesses how well our subsidiaries apply and comply to 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. First to check 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. In 2016 assessments we saw all subsidiaries making significant improvements in the maturity level of their controls for the LEA guidelines, with all but one reaching the highest maturity level.

A 'Major events' Guideline was approved by the LIP Committee in Q3 2015. It defines 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 TID and the GNI.

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.

> "In 2016, we began work on an aligned global privacy policy framework. Millicom's EC approved broad privacy principles for the company and guidelines and supporting decision guides were created for commercial teams on customer privacy issues. The work continues to bring more transparency to Millicom's privacy policies and practices."

[21] http://www.millicom.com/media/3859122/GUIDELINE_Law-Enforcement-Assistance-MILLICOM-2015.pdf

9. 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 are a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy and this year we will join 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 donations agreement with international human rights organization Civil Rights Defenders to increase bilateral sharing of information on situations in our markets and to create links with local human rights defenders.

Concurrently, we engage directly with in-country government and other stakeholders on the topic as much as possible. Discussion are held with Ministers of Interior and Security, as well as ICT, and relevant Security Services, so as to enhance their understanding of our obligations also outside of their countries, while repeatedly also highlighting the reputational risks for their government and foreign investment possibilities. We also discuss these topics regularly with relevant diplomatic representatives.

International financial institutions

One of the key topics of engagement for Millicom has been 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 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. We have an on-going relationship with the agency, having met in May 2016 and having undergone a due diligence by SEK for specific investments.

The SEK/EKN consulted Millicom and its peers in the Telecommunications Industry Dialogue (TID), for input on a paper being drafted in conjunction with the Institute for Human Rights and Business.

Telecommunications Industry Dialogue (TID)

Millicom is one of the founding members of the TID on Freedom of Expression and Privacy, a joint industry group working since 2011 on principles, tools and joint advocacy on privacy and freedom of expression challenges. Millicom's VP of Corporate Responsibility is a TID Board member and chaired the initiative in 2014-2015. Other members include AT&T, Nokia, Orange, Telefonica, TeliaCompany, Telenor, and Vodafone. In 2016, TID met quarterly face to face and every other week over the phone. We strongly advocated TID to merge with the GNI , and in the beginning of 2016, we together with six other members of the TID joined the GNI as observer members for a one-year period. That period will end in March 2017, when Millicom and other members of the TID will be formally joining the GNI.

> At Millicom, we believe that our ability to affect legislation or challenge 'major events' is greatly increased by joint efforts with others. In 2016, we became observer members of the Global Network Initiative with a view for full membership in 2017."

Global Network Initiative (GNI)

At Millicom, we believe that our ability to affect legislation or challenge 'major events' is greatly increased by joint efforts with others. In 2016, we became involved as observers in the GNI's committee and policy work, sharing of 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 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 this continued collaboration during 2017 as full members, 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.

Consultations with UN Special Rapporteur

Millicom engaged with the UN Special Rapporteur (SR) on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, on a number of instances last year. In February 2016, Millicom participated at a consultation with the private sector in Geneva on responsibilities of the ICT sector with regards to freedom of opinion and expression. We then had a follow up meeting with the SR at a 'brainstorming session' held by Article 19 in London in July and participated at a further expert consultation session held by the University of Connecticut in October. Later in the year, Millicom helped provide formal written feedback to the SR together with other TID companies.

Freedom Online Coalition

Millicom regularly speaks at events relating to the topic of privacy and freedom of expression. In 2016, we participated in several panels at the Freedom Online Coalition in Costa Rica. The Freedom Online Coalition is a partnership of 30 governments, working to advance internet freedom. The Coalition provides a platform for multi-stakeholder engagement, engaging with civil society and the private sector in a dialogue on pressing issues related to digital rights. Millicom's VP of Corporate Responsibility and Millicom's Corporate Responsibility Manager for Latin America spoke at five panels on issues ranging from network shutdowns to children's right to privacy and to transparency reporting.

10. Implementation of TID Guiding Principles

Table 16

Principle	Where to find Millicom's progress in this report
1. Create and/or maintain relevant policies, with Board oversight or equivalent, outlining commitment to prevent, assess, and mitigate to the best of their ability the risks to freedom of expression and privacy associated with designing, selling, and operating telecommunications technology and telecommunications services;	See section 8.
2. Conduct regular human rights impact assessments and use due diligence processes, as appropriate to the company, to identify, mitigate and manage risks to freedom of expression and privacy – whether in relation to particular technologies, products, services, or countries – in accordance with the Guiding Principles for the Implementation of the UN 'Protect, Respect and Remedy' framework	See section 8.
3. Create and/or maintain operational processes and routines to evaluate and handle government requests that may have an impact on freedom of expression and privacy	See section 6 and 8.
4. Adopt, where feasible, strategies to anticipate, respond and minimise the potential impact on freedom of expression and privacy in the event that a government demand or request is received that is unlawful or where governments are believed to be mis-using products or technology for illegitimate purposes	See sections 1, 2 and 6-9.
5. Always seek to ensure the safety and liberty of company personnel who may be placed at risk	See sections 1, 2, 6, and 8.
6. Raise awareness and train relevant employees in related policies and processes	See section 8.
7. Share knowledge and insights, where relevant and appropriate, with all relevant and interested stakeholders to improve understanding of the applicable legal framework and the effectiveness of these principles in practice, and to provide support for the implementation and further development of the principles;	See section 9.
8. Report externally on an annual basis, and whenever circumstances make it relevant, on their progress in implementing the principles, and as appropriate on major events occurring in this regard	This full report.
9. Help to inform the development of policy and regulations to support freedom of expression and privacy including, alone or in cooperation with other entities, seeking to mitigate potential negative impacts from policies or regulations	See section 9.
10. Examine, as a group, options for implementing relevant grievance mechanisms, as outlined in Principle 31 of the UN Guiding Principles for Business and Human Rights.	See section 9 and our work with the TID and GNI.

Millicom
For further information please contact:
CR@millicom.com

millicom.com

Designed by
FleishmanHillard Fishburn
www.fhflondon.co.uk

MILLICOM
THE DIGITAL LIFESTYLE