MILLICOM
THE DIGITAL LIFESTYLE

Law Enforcement Disclosure Report

2015

Contents

1. Introduction

The topic of privacy and freedom of expression has been under increasing, and intense, scrutiny in the public domain in recent years. Edward Snowden's information leaks, subsequent revelations of NSA surveillance programmes and situations where telecom companies have been accused of complicity with governments to spy on their citizens, have resulted in increased focus on, and increased reputational risk associated with, requests from law enforcement for surveillance and customer data for any company providing communications services.

Public attention has also resulted in ethical investors and other stakeholders increasing their scrutiny of telecom operators' readiness to manage such requests and related risks. These stakeholders expect us to be a contributor to the societies in which we do business, and to operate with a focus that goes beyond short-term financial returns and includes also human rights and similar considerations.

These expectations, however, are completely compatible with the operation of a profitable business, particularly as we take a longer-term view. To remain profitable, we want as many people to use our services as possible. To permit this to happen we need our customers to trust us to keep their information safe.

We must have processes in place to identify our impacts and understand how our actions may affect human rights of our customers or our wider operating environment and how to minimise potential negative impacts.

We are foreign investors, who build critical communications infrastructure and provide access to telephony and internet services under licenses and spectrum granted by national governments.

Accordingly, we must respect local laws and are legally bound to support governments in their legitimate duty of protecting public safety and security.

We have a duty to keep our employees and others who work with us to provide our services safe, and we need to protect the physical assets – radio towers and transmitters, shops and offices – that we rely on to provide our services.

All the above considerations underpin our decisions when we receive demands from law enforcement agencies, and are fundamental aspects of the discussions around company responsibility in protecting freedom of expression and privacy of citizens.

Telecommunications is a vital tool for governments to help protect public safety and security. For these same legitimate reasons, governments and law enforcement authorities from time to time request access to communications data of our customers. The ITU Constitution[i] includes articles on the stoppage of telecommunications, the suspension of services and the secrecy of telecommunications. International conventions state, however, that any such action or access must have a legal basis, it must be proportionate to the perceived threat, and it represents an exception or limitation to freedom of expression or privacy of individuals.

It is our responsibility to challenge requests we receive from governments that do not follow what international conventions[ii] demand. Never, however, are the decisions to do so straight-forward and simple.

We hope this report will help readers understand the context in which we operate telecommunications networks and interact with law enforcement agencies.

Luxembourg, March 2016

Rachel Samrén
EVP, External Affairs

Salvador Escalón
EVP, General Counsel

2. What we are reporting, not reporting and why

We are publishing this report for two key reasons: to respond to stakeholders who have asked us to be more transparent about how we deal with government requests and because we want to advance the understanding of the real challenges and situations telecommunications companies face and the contexts in which we have to make decisions relating to government requests.

We hope that this report will support 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 what types, and how many law enforcement requests we receive, and more importantly we describe the overall context in which they are made. 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 a number of specific 'major events' we have faced during the year. Whenever possible we disclose the countries in which they took place.

> We want to advance the understanding of the real challenges and situations telecommunications companies face and the contexts in which we have to make decisions relating to government requests.

In line with the commitments that we have made to implement the Telecommunications Industry Dialogue (TID) ten principles[iii] 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 to our customers' freedom of expression in 'major events' situations.

What we are not reporting?

Law enforcement requests are by definition sensitive requests. 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, such situations have strict confidentiality requirements and potential sanctions attached to them which mean that often we are forbidden by law from disclosing details of the requests we receive. In some cases we are explicitly told not to disclose any details of specific requests.

> Clear laws that respect international conventions and narrowly define by who, how and in what circumstances law enforcement requests can be made are crucial to protect privacy and free expression.

It is also often difficult for us to discuss publicly how we engage with law enforcement or the authorities, or the ways we may try to challenge their approach. This is a source of frustration at times, and may lead to incorrect perceptions of apparent inaction. In this report we purposefully describe our engagement in more broad terms rather than in relation to specific events for the aforementioned reasons.

We are not disclosing the numbers of government requests by country as some of our peers have done.

The reasons for this are multiple. We operate in some countries where publicly disclosing such numbers may put the safety of our employees at risk. In some countries discussion with the authorities regarding disclosure of such issues might be negatively received.

Accordingly, for the purposes of this report, we have decided not to engage the authorities to seek their approval for publication of country-specific details. Rather we have focused our resources this year on improving our internal processes and understanding the issues so as to support such engagement going forward.

In this report, we aggregate numbers of requests on a regional level, which continues our improvement on previous years when we have published the overall range of requests.

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. Legal frameworks and law enforcement capacity

We only disclose information of our customers to third parties in accordance with the law. As requests are received, our legal teams are the first to make an assessment of requests and give their view on whether a request follows local due process.

In 2015 we completed a mapping exercise of legal frameworks and government powers for surveillance, content blocking and service shut downs that exist in each of our operations, identifying the exact laws and acts by which local operations must abide. This can be a surprisingly complex exercise as often such powers are not defined in single texts but found inside several separate pieces of legislation.

This information is now centrally stored and can be accessed by Millicom's legal staff and members of the company's Lawful Interception Policy Committee (see more information about the Committee on page 10). The information is, and will be, of significant support for speeding up legal reviews. Having this information available at global level also helps us support the local teams in specific situations.

Information about the legal frameworks from four of our operations (Colombia, DRC, Ghana and Tanzania) has been published as part of the joint legal frameworks research of the TID[iv]. We look forward to publishing the same information on more of our operations in 2016.

Overall legal landscape

In general we experience some challenges with clarity of rule of law, absence of legal oversight or separation of powers in our operating environment. This also applies to laws and processes for surveillance.

The mapping of legal frameworks reveals that only a few of the countries in which we operate have clear laws and processes on who, how and in what circumstances is allowed to make requests for surveillance, customer data or service suspensions. In many countries particularly the laws relating to emergency and national security powers of the authorities are very broad.

Sweeping or non-specific laws in essence mean that in emergency situations (which are themselves not clearly defined) the authorities in some countries are within their powers to ask for extreme responses 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.

Decisions to challenge 'major events' requests are rarely simple. In essence we would be breaking local law by challenging requests that have a legal basis – even when the sweeping nature of those laws can be questioned. We must consider direct consequences for our local management if sanctions are applied. Sanctions do not limit themselves to fines, but can in some cases also include imprisonment. Often these requests happen during a particularly volatile time of civil unrest, which means we must consider safety risks to our staff as well as potential retaliation from the general public against our company and our visible assets, such as shops and base station sites.

There are situations where legal processes that do exist are not respected. The more specific and precise the law is on exactly by whom, how and in what types of situations requests are permitted, the more straightforward it is for us to analyse the legality of the request – and provide clear grounds on which to reject requests that do not follow due process.

We routinely reject requests for customer metadata that do not come from authorised parties, that are not made in the written format described in law, or that request information in cases where the request of such information is not justified. An example of the latter would be receiving a judicial request for customer data in a divorce case, when the law specifies that such data can only be requested for the most serious crimes, such as homicides or drug-related crimes.

All of our countries of operation rank as high risk in Transparency International's corruption perception index. Corruption in the judiciary system may make the assessments of the legal validity of the requests difficult, as requests may appear legally valid, even when they are not. An example of this would be when correct documents are provided that have been obtained by the requestor through unlawful means. To address this, we have in some countries asked the authorities to strictly limit the individuals in the judiciary system who may sign off requests.

Cost of interception and managing law enforcement requests

The laws or license requirements in most of our markets require that we bear the cost of purchase and installation of any lawful interception equipment. Laws usually define technical requirements for such equipment to be aligned to the main international standards for lawful interception. To our knowledge all equipment installed by us conforms to ETSI, 3GPP or CALEA standards.

Unlike in many developed countries, we are not compensated at cost for the resources we need to have in place for assessing and processing requests from law enforcement.

Capacity of local law enforcement

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

All of this potentially creates tension between our local operations and law enforcement, uses management time and creates additional costs.

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 a country to promptly retrieve it.

We would welcome more technical assistance to developing countries from the international community in the area of cyber-investigations, as well as in designing transparent and clear laws around surveillance.

Advocating for clear laws

Clear laws that respect international conventions and narrowly define by whom, 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.

Clear laws and processes are also crucial tools for telecommunications companies to respect privacy and freedom of expression of our customers.

This is not because we feel that our responsibility starts and ends with the law, but because clear laws promote accountability for all parties.

Advocating and helping to define what is clear surveillance law is an area we will focus more on going forward. We are encouraged by the fact that the Freedom Online Coalition has established a working group on this subject, and we will focus on leading work in this area for the TID in 2016.

4. Requests from law enforcement in 2015

Definitions of different types of requests

As other law enforcement disclosure reports by our peers have pointed out, there are no agreed or standardised definitions or ways to classify law enforcement requests. At Millicom, we classify requests into three distinct categories: requests for interception; customer metadata; and customer financial data (relating to the mobile financial services or mobile money services we provide). Some of our 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 count as 'major events' and they are described in the next section.

Definitions for the three categories

Category	Definition
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, past call, SMS, email traffic, Internet traffic information, or documents from cloud services, or requests for location information (base station or GPS information).
Requests for Mobile Financial Services (MFS) related data	Information relating to MFS, such as confirming an individual is an MFS customer, transaction data and other account activity. These requests do not always relate to financial crime.

Numbers of requests in 2015 in our regions

In some countries data collection on law enforcement requests remains challenging. This is particularly the case in our markets in Africa, where due to the relatively low number of requests received, no specific software is used to record and process requests.

In 2015 we created a dedicated reporting template for those operations that did not have specific tools in place to record the time, origin and category of each request. The teams are also requested to log requests that have been rejected and the reasons for their rejection.

Data collection still remains manual in most countries and hence human error in data collection cannot be ruled out. We plan to include this data into the scope of our non-financial reporting assurance within the next two years. For the time being a data quality check is done internally as part of our non-financial reporting process.

Last year we reported a general range of request volumes. This year we are reporting requests in the above-mentioned three categories by region.

We believe, that what we disclose gives a good picture of the different levels of law enforcement activity towards communications service providers in the two regions, and allows comparison of these volumes with those seen in more developed markets.

Noting how much lower these figures are to some published in the USA or Western Europe, it seems likely that the volumes of demands on ICT companies such as Millicom will continue to rise in Latin America and Africa.

Numbers of requests by region and category

	Interception	Metadata	MFS
Latin America	184	33,100	262
Africa	5	5,513	354

Data from seven countries in Latin America and six countries in Africa.

The actual written request any operation receives counts as one request in the above table. 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 first 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 on more than one suspect'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. There is an increase in the number of requests that our operations have reported to us compared to 2014. This may also be in part the result of the improved recording of requests.

Rejected requests

In countries that have systematically recorded the number of requests they reject, the number varies from 3-5% 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 occasions are made by parties who, by law, are not allowed to make them or are made without the proper judicial oversight.

Direct access

To the best of our knowledge, in five of our markets law enforcement authorities have direct access to our network. This means that the authorities are able to intercept communication of our customers without our knowledge or involvement.

In most of these cases, clear judicial oversight exists where law enforcement is only able to intercept with the permission of a judicial order. There are further oversight mechanisms or human rights committees in place overseeing the overall use of these powers in at least two of the five countries.

5. Cases – description of 'major events' in 2015

We call requests falling outside of normal law enforcement assistance requests 'major events'. All local operations are required to escalate these events to global management and take a number of steps in order to minimise the effect of such events on our services. You will find more details on this process in section 8.

The events described in this section are those that were reported to global headquarters in 2015. While we are confident that this gives a representative picture of the nature and number of such events in our markets, it is possible that there have been other events we were not made aware of.

'Major events' can include requests for shutdown 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[v], denial of access for specific individuals, significant changes relating to surveillance techniques or operational processes (direct access or 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 2015, we had a total of 20 events falling into the definition of major events. Five of these were events carried on from 2014. Fourteen of the events were in Africa. The events can be broken into the following categories:

Category	
Shutdown of services	8
Proposal for significant changes in local laws	3
Proposal for significant changes in technical or operational procedures	3
Interception or customer data requests outside of due process	2
Politically motivated messages	2
Other	2

As with law enforcement requests, there are no accepted or standardised definitions for different types of major events or how they should be accounted for.

In Millicom's case, we count the number of actual requests that have been made directly to us. One request may include a shutdown of several different services, or request to shut down parts of the network in several different geographical areas.

In practice this means that, for example, for a request of a shutdown of cell towers around prisons in Central America, we count one request per country instead of the number of prisons or cell towers that have been shut down.

Shutdown of services

The security situation in our Central American operations has continued to be challenging in 2015.

Since 2014, authorities in Guatemala, El Salvador and Honduras have enacted laws that oblige all telecom operators to shut down services or reduce signal capacity in and around prisons, as authorities suspect that crime gangs continue to operate from inside prisons by using cell phones that have been smuggled onto the premises. Telecom operators were originally requested to shut down base station towers that serve large areas, also affecting populations living in the vicinity of the correctional facilities as well as disrupting everyday activity, such as the use of ATMs.

We have and continue to actively engage with the authorities and industry peers, focusing on finding alternative solutions that would address the issue in ways that would 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 the relocation of prisons outside of densely populated areas.

At the end of 2015, in Guatemala and Honduras all prison blocking of cell phone signals was done in a more targeted manner affecting only the inside of the prison buildings, using jammers or 'dummy cells'.

Apart from the prison shutdowns above, in 2015 all other requests for shutdowns were received in our African operations. There is little we can disclose on these requests due to legal restrictions.

In January 2015, our local operation in DRC was requested to suspend all internet and SMS services in the country with immediate effect.

The request was made under the DRC Framework Law (Article 46) that gives the government powers to prohibit all or part of the use of telecommunications for reasons of public security and for a period that they may determine. Our customer service network immediately informed our customers of the situation.

5. Cases – description of 'major events' in 2015 (continued)

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.

In the DRC case, we were able to swiftly align with all industry peers on a common message to convey to our customers on the shutdown that accurately described the situation. This is not always possible.

There are occasions where we are specifically instructed by the authorities not to disclose that a governmental requests is at the origin of a shutdown. In these cases, we 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.

There have been cases where we have been explicitly told to inform our customers that we have a technical fault in the network. In such situations we engage in dialogue with governments with the aim of ensuring that factual information can be provided to the customers in as prompt a manner as possible.

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 developments around local legal frameworks in both of our regions.

In April 2015, Tanzania adopted its new Cybercrime Act 2015, which was immediately widely criticised by human rights groups. The government has agreed to carry out a review of the Act as a result, but to our knowledge this has not yet taken place. In June, the Paraguayan Senate rejected the controversial "Pyrawebs" data retention bill which had received wide-ranging opposition, mostly on grounds of human rights concerns. At the end of the year, the Ghanaian government introduced a proposal for a new Interception of Postal Packets and Telecom Messages Bill. The bill is to go in front of the Ghanaian Parliament in 2016. Millicom has submitted extensive comments to the bill jointly with the industry. The bill has also received feedback from civil society and opposition parties, who have criticised Parliament for allowing only a short consultation period[vi].

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 recognising that all acts of interception and data requests represent exceptions to fundamental rights as outlined in international human rights law and relevant conventions.

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 benefit the local government only, they should be borne by the government, also in order to encourage the proportionate use of such powers.

> The most common feedback we give to legislators is for establishment of judicial oversight, promotion of proportionate and necessary measures, and the importance of recognising that all acts of interception and data requests represent exceptions to fundamental rights as outlined in international human rights law and relevant conventions.

Interception or customer data requests outside of due process

We described in the previous section that we reject a number of requests each year as they do not follow local due process. Within the major events category we classify separately requests for interception or customer data that do not follow local due process and which in addition are clearly politically motivated or disproportionate.

In 2015, we are aware of two such requests, one in Latin America and one in Africa. One requested personal contact information of our entire customer base in a specific region for purposes, we believe, of political advertising. Another requested open-ended interception of communications of a group of individuals. Our local operations did not adhere to the request in either case.

Politically motivated messages

There are cases where our services are requested to be used for political purposes. In a positive development we, in 2015, worked together with our peers and the telecommunications regulator in relation to the Presidential elections in Tanzania to define clear rules for any political campaigning via SMS, in particular with a view to ensure prior consent of message recipients.

In another instance we were requested to send messages to support a specific political cause. We did not carry out the request.

Other requests

In 2015, other requests that we have classified as major events have taken place around specific events in Africa. We were requested to have additional resources available for a specific period of time to be able to promptly respond to a potential increase in law enforcement requests on an election weekend. We made resources available but no requests were made. The other request relates to a national security situation, details of which we are unable to disclose due to legal restrictions.

6. Trends and priorities for 2016

Trend in our operating environment

In 2015, we saw a significant increase in 'major events' in our markets. In part this is because we are more aware of such situations on the ground due to a more structured approach to handling these events and the implementation of a clear escalation process.

It has also been a tumultuous year in many of our markets. As previously mentioned, organised crime and related gang violence has significantly increased in Central America. Africa has experienced an increase in terrorist incidents. Several suicide bombings were carried out in Chad during the year, and the country is engaged in military action against Boko Haram.

Presidential elections were held in two of our markets in 2015 – a further three will take place in 2016. Three of our operations – DRC, Rwanda and Bolivia – proposed or made changes to the constitution relating to presidential mandates.

We have seen an increase in requests for shutdowns, in Africa in particular. Shutdowns are requested either for basic SMS messaging services, for popular social media services such as Facebook, Twitter, Viber and WhatsApp, or in the most extreme cases for all of the internet. These can last from one day to several weeks at a time.

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[vii], shutdowns seem to be on a rising trend in the region. Complete or partial shutdowns also took place in several other African countries where we did not operate, and this trend continues across Africa in 2016.

There are many things we can do – and do – as an industry to attempt to limit both the scope and duration of such shutdowns. We engage with governments during and outside of specific volatile situations to discuss consequences of these actions, and have been able to have open and frank conversations.

> 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 seem to be on a rising trend in Africa.

We have been sharing our experiences of shutdowns in several forums in 2015. Good work was done in 2015 by the Institute of Business and Human Rights on the impact of such shutdowns in Pakistan[viii]. This is a topic we have discussed on several occasions with our peers in the TID, sharing best practices. We hope that with our observer status 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 the engagement process with governments.

However, it needs to be remembered that governments are ultimately accountable for shutdowns. A strong joint response from the international community is needed to put a stop to this trend, which also affects people's right to peaceful assembly.

We have been calling 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 agency, EKN, in this area.

Priorities for 2016

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 Global Network Initiative to see how we can jointly address some of the challenges.

We will work on defining clear laws with TID and other stakeholders, as we expect that the trend we have seen in 2015 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 the current legal frameworks of more countries in 2016 together with the 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.

Internally, we will continue to strengthen the implementation of our existing guidelines for law enforcement assistance requests and major events. We are also in the process of building a wider framework on digital rights with a separate cross-functional team.

7. Our internal policies, guidelines and governance

Millicom recognised at an early stage the need to engage proactively on privacy and freedom of expression to better manage risks relating to it.

We have taken several steps to minimise 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 2015, the Government Relations and Corporate Responsibility Committee of the Board requested a detailed report on Millicom's risk exposure in relation to privacy and freedom of expression and current mitigation measures.

Board and management committees – governance

All corporate responsibility activities in Millicom are overseen by the Government Relations and Corporate Responsibility Committee of the Board of Directors (GRCR Committee). The Committee is chaired by Dame Amelia Fawcett and has three permanent members. Millicom's CEO and EVP of External Affairs are permanent guests, and heads of corporate responsibility and regulatory affairs are invited to give updates in their specific functional areas. The Committee meets every quarter and advices management on specific issues and approves the company's overall strategic Government Relations and Corporate Responsibility approach.

In 2015, the GRCR Committee requested a detailed report on Millicom's risk exposure in relation to privacy and freedom of expression and current mitigation measures. The Committee advised Millicom to continue its strong proactive approach and to deepen relationships with civil society on a country level.

In January 2014, to better co-ordinate 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 External Affairs, VP Security, EVP and General Counsel, Director of Communications, Director of Compliance and Business Ethics, COO MFS and Investigations Manager. The Group meets quarterly 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 2015.

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[ix], 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[x] 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.

Millicom Group Guideline for Law Enforcement Assistance Requests (LEA Guideline) was finalised and approved by the LIP Committee in Q1 2015. It clearly outlines our obligations within international frameworks, the 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[xi].

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. First controls were carried out in 2015.

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 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 on July 1, 2015. Full compliance across the Group is expected by December 2016.

All Millicom employees must take Information Security training, which addresses the importance of protecting customer data. The training material is available at our eLearning platform, Millicom University, and is mandatory training for all employees. New employees must complete the IS training within 90 days of job commencement, and IS awareness materials are distributed to all employees at least annually.

8. Our engagement

Membership in Telecom Industry Dialogue on Freedom of Expression and Privacy

Our ability to affect legislation or challenge 'major events' is greatly increased by joint efforts with others.

All communications companies face these same challenges. We are one of the founding members of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy (TID), a joint industry group working since 2011 on principles, tools and joint advocacy on privacy and freedom of expression challenges. Millicom VP of Corporate Responsibility is a TID Board member and chaired the initiative in 2014-2015. Other members include Vodafone, Orange, Telefonica, AT&T, Nokia, Alcatel-Lucent, TeliaSonera, and Telenor.

> We would welcome more technical assistance in developing countries from the international community in the area of cyber-investigations, as well as in designing transparent and clear laws around surveillance.

In 2015, TID met quarterly face to face and every week over the phone. We strongly advocated joining Global Network Initiative and TID, and at the beginning of 2016, we announced with six other members of the TID that we had been accepted as observer members of the GNI for a one-year period, with the aim of becoming members in 2017.

Joining the GNI will allow us to fully participate in what we consider to be a critical debate with more than 50 organisations, human rights experts, investors, academics and internet companies.

In 2016, we look forward to engaging in the GNI's 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.

Other engagement

Millicom regularly speaks at events relating to the topic. In 2015, we participated in a panel at the Stockholm Internet Forum in October, spoke at an investor event by GES in London in May, and presented our work in three stakeholder meetings organised in conjunction with TID quarterly meetings. In these events, our focus has been on bringing the significant and specific challenges posed by operating in emerging markets, in e.g. law enforcement capacity, into the debate.

In February 2016, Millicom was invited by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, to a consultation with the private sector on responsibilities of the ICT sector with regards to freedom of opinion and expression.

In response to the recommendation by our GRCR Committee, at the end of 2015 we signed a three-year donations agreement with international human rights organisation Civil Rights Defenders to increase bilateral sharing of information on situations on the ground in our markets and to create links with local human rights defenders.

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

References

[i] TU Constitution: ARTICLE 34 – Stoppage of Telecommunications, ARTICLE 35 – Suspension of Services, and ARTICLE 37 – Secrecy of Telecommunications.

[ii] Universal Declaration of Human Rights (UDHR), Article 12, and in the International Covenant on Civil and Political Rights (ICCPR), Article 17. The right to freedom of opinion and expression is enshrined in the UDHR, Article 19, and the ICCPR, Article 19.

[iii] http://www.telecomindustrydialogue.org/about/guiding-principles/

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

[v] With the exception of blocking of child sexual abuse content, which in 2015 took place only in Colombia.

[vi] http://pulse.com.gh/telecom/postal-packets-and-telecommunication-messages-bill-government-to-spy-on-you-with-new-law-id4694687.html

[vii] Joint Declaration on Freedom of Expression and Responses to Conflict Situations: http://www.osce.org/fom/154846

[viii] Security v Access: The Impact of Mobile Network Shutdowns https://cihr.eu/wp-content/uploads/2015/09/2015-09-Telenor-Pakistan-Case-Study.pdf

[ix] http://www.millicom.com/media/3817997/millicom_code_of_conduct_doublepage.pdf

[x] http://www.telecomindustrydialogue.org/about/guiding-principles/

[xi] Millicom Group Guideline for Law Enforcement Assistance requests http://www.millicom.com/media/3859122/GUIDELINE_Law-Enforcement-Assistance-MILLICOM-2015.pdf

MILLICOM

THE DIGITAL LIFESTYLE

www.millicom.com