GSMA

Assessing the impact of telecoms traffic monitoring systems in Sub-Saharan Africa

October 2022

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Follow the GSMA on Twitter: @GSMA

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

@GSMAi

Published October 2022

Author
Kenechi Okeleke, Director, Regional, Social and Policy Research

Contents

Executive summary

Telecoms infrastructure is fundamental to the economy and widely recognised as the backbone of the digital transformation of society. Telecoms networks enable the provision of vital services that improve lives by supporting the development of an inclusive digital society. They have been instrumental in ensuring continuity of business and essential services during the Covid-19 pandemic and are playing a crucial role in the recovery phase too. The use of telecoms networks generates a huge amount of traffic data with a number of attributes, including information on the routing, timing, duration and volume of communications conveyed over the network.

In Sub-Saharan Africa, several national governments and regulators have adopted technical solutions that involve the installation of external equipment in telecoms networks by a third-party vendor to monitor telecoms traffic data. These telecoms traffic monitoring systems (TTMSs) can actively or passively collect, record or tap into content of incoming and outgoing electronic communications traffic in real-time and store or report this information to the telecoms regulator or other authority.

The reasons presented by national governments and regulators for implementing these systems include the following:

- to prevent SIM box fraud
- to verify revenues due to the government from the provision of telecoms services
- to provide real-time visibility of traffic on various telecoms services.

Recent years have seen the expansion of the scope of TTMS platforms in some countries – beyond the original intent to block grey international voice traffic, to now include the monitoring of SMS volumes, national on-net and off-net voice traffic, data usage and mobile money transactions.

The GSMA has conducted a survey of national regulatory authorities (NRAs) and mobile operators in Sub-Saharan Africa to understand the impact of TTMS implementations in the region. The survey and other available evidence show the following:

- International traffic volumes have declined in most cases, partly driven by the imposition of the surtax on international inbound call termination (SIIT). This means that revenue uplift expectations from the implementation of TTMS have not been realised.
- The cost-benefit trade-off for TTMS platforms is rather weak, considering the cost of initial deployment and ongoing maintenance of the systems. The information they provide can already be sourced in more efficient and cost-effective ways using existing means. Meanwhile, where operators bear part or all of the initial and/or maintenance costs of TTMS platforms, this forms an additional burden, with direct consequences for consumers in terms of affordability and quality of service (QoS).

- The risk to customer data privacy and telecoms network security is high. TTMS platforms often allow external systems and non-state actors access to sensitive data and network infrastructure. The sensitivity of telecoms infrastructure and data underlines the need for authorities to adopt the right approach to collecting, processing and storing network data.

Insights from the survey and the assessment of the impact of TTMS platforms show that the associated costs and risks outweigh the benefits. Consequently, governments need to reassess their approach to telecoms traffic monitoring, with a view to utilising secure, more efficient and cost-effective methods in line with international best practices.

Best practices and alternative approaches to telecoms traffic monitoring

- **Use more efficient methods for network traffic and revenue verification** – Governments should equip the relevant agencies with the right skills and tools to carry out revenue assurance duties on behalf of the government. These agencies already have a statutory right to conduct the required audits and should be used for that purpose.

- **Work with operators to fight and curb fraudulent traffic** – Best practices around the world are based on cooperation and trust between operators and regulators, as well as information and insight sharing to improve QoS and tackle SIM box fraud. Indeed, operators continuously invest in monitoring, control and investigation solutions to fight fraud, in line with the objectives of national authorities.

- **Work with operators to extract relevant traffic data** – Where governments need traffic data (e.g. for planning purposes and to gain insights into the digital economy), they should work with operators to agree a feasible mechanism to access the data required, in line with established data security and privacy standards.

- **Protect citizens' data** – Governments must recognise the risk of giving unfettered access to sensitive network data to non-state actors, and the implications for national security and customer data privacy. The attractiveness of a TTMS platform as a target for hostile nation states or other malicious actors to exploit in order to undermine national security should not be underestimated.

- **Base decisions on evidence** – Claims regarding revenue leakages, without the necessary studies or evidence to establish their veracity, are unfounded and unjustified. Furthermore, accusations of misreporting result in reputational damage for operators and mistrust among stakeholders.

- **Ensure a level playing field for all sectors** – The telecoms sector should be treated no differently to other sectors; more stringent revenue assurance requirements end up placing an additional burden on operators.

- **Avoid expanding the scope of existing systems** – Extending TTMS to other services poses significant technical and operational challenges for operators, including exposing the network to cyberattacks by weakening the security systems established by operators.

1. Context: TTMS in Sub-Saharan Africa

Telecoms networks have become an essential part of daily life, enabling people to stay connected and access life-enhancing services. The Covid-19 pandemic has underlined the importance of telecoms networks to society. People have relied on connectivity for work, learning, entertainment and many other services amid social and travel restrictions. The use of telecoms networks generates a huge amount of traffic data with a number of attributes, including information on the routing, timing, duration and volume of communications conveyed over the network.

The sensitive nature of telecoms traffic data with regards to data security and customer privacy means that collecting, processing, sharing and storing such data is usually subject to strict data protection guidelines. For example, the Privacy and Electronic Communications Regulations (PECR), which is the UK's version of the EU e-Privacy Directive,[1] stipulates that network operators can only process traffic data to manage billing and traffic on their networks, handle customer enquiries and prevent/detect fraud. Traffic data can also be used to market electronic communication services and provide a 'value-added service', but with consent from the subscriber, while the NRA or another public agency that has statutory authority can request traffic data for specific purposes – for example, to resolve disputes.

Besides the collection and processing of traffic data for permissible reasons, a number of countries have adopted technical solutions that involve the installation of external equipment in the telecoms network by a third-party vendor to monitor telecoms traffic data. These telecoms traffic monitoring systems (TTMSs) can actively or passively collect, record or tap into content of incoming and outgoing electronic communications traffic in real-time and store or report this information to the telecoms regulator or another authority.

TTMS platforms are most prevalent in Sub-Saharan Africa; only a handful of countries outside the region (such as Pakistan[2] and Bangladesh[3]) have adopted some form of third-party traffic monitoring solution. Elsewhere, particularly in developed countries and regions, telecoms regulators rely on reporting by network operators, within established data security and privacy guidelines, to collect and process telecoms traffic data.

Some TTMS implementations have challenged the conventional architecture of telecoms networks and their operations with regards to the routing of traffic – for example, connecting beyond the point in the network where the operator's billing systems are connected and introducing monopoly gateways for local and international network traffic.

[1] https://www.legislation.gov.uk/uksi/2003/2426
[2] "Pakistan moves to install nationwide 'web monitoring system'", Codastory.com, October 2019
[3] "Bangladesh to set up telecom monitoring system", Developing Telecoms, August 2021

In the late 2000s, Ghana and the Republic of the Congo announced their intentions to implement TTMS platforms. Since then, several other governments and regulators across the region have also announced plans and, in some cases, proceeded to implement TTMS platforms in their respective markets (see Figure 1). The main objective was to monitor international inbound and outbound voice traffic and prevent SIM box fraud perpetuated by the use of illegal voice-over-IP (VoIP) gateways to terminate international traffic.

Recent years have seen TTMS platforms in some countries expand in scope beyond international voice traffic to include the monitoring of SMS volumes, national on-net and off-net voice traffic, data usage and mobile money transactions. As over-the-top (OTT) services become prevalent, some national regulators envisage the enhancement of TTMS platforms to eventually capture OTT traffic and possibly monitor social media content.[4]

Figure 1: Current state of TTMS implementations in Sub-Saharan Africa

Country	Status	SIIT?
Angola	Live	No
Cameroon	Live	No
Chad	Live	Yes
Congo	Live	Yes
DRC	Planned	Yes
Gabon	Live	Yes
Gambia	Planned	Yes
Ghana	Live	Yes
Guinea Bissau	Live	Yes
Guinea	Live	Yes
Lesotho	Planned	No
Liberia	Live	Yes
Mozambique	Live	Yes
Nigeria	Planned	No
Rwanda	Live	Yes
Sao Tome	Planned	Yes
Senegal	Live	No
South Sudan	Live	No
Tanzania	Live	Yes
Zambia	Live	No
Zimbabwe	Live	No

Note: SIIT – surtax on international incoming traffic
Source: GSMA

[4] Key informant interview

Examples of recent TTMS developments in Sub-Saharan Africa

Zimbabwe – In June 2022, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) commissioned a TTMS platform to monitor network traffic data.[5] The government expects the system to help tackle SIM box fraud and provide revenue assurance and traffic data in real-time.

Lesotho – In June 2021, the Lesotho Communications Authority (LCA) opened a public consultation on the proposed Compliance Monitoring and Revenue Assurance Regulations, 2021. If approved, the regulations will pave the way for the installation of a TTMS called the Compliance Monitoring and Revenue Assurance Tool (C-MART), which will monitor traffic data and mobile money transactions.[6]

Guinea – In April 2021, telecoms regulator ARPT signed a five-year contract with Global Voice Group (GVG) to deploy its mobile and digital ecosystem regulation platform to monitor mobile and digital identities, interconnectivity, data services and mobile money.[7]

Angola – In March 2021, the government of Angola announced that a TTMS platform, called the Gateway International Angola (GIA), would start signing contracts with telecoms operators. The platform was implemented through a public-private initiative with Swiss company MGI.[8]

Tanzania – In January 2019, GVG transferred its TTMS to the Tanzania Communications Regulatory Authority (TCRA). In addition to international traffic, the system monitors end-to-end transactions, customer recharge, roaming and mobile money services.[9]

Ghana – In October 2018, the government in Ghana launched the Common Management Platform (CMP) for telecoms supervision – a TTMS built by Kelni GVG that will allow the National Communications Authority to monitor international traffic. In February 2021, the government announced that the platform will be upgraded to monitor mobile money transactions and provide other digital services.[10]

[5] "Equipment to track telecommunications services usage now in place in Zimbabwe", Bulawayo24.com, June 2022
[6] Lesotho Communications Authority
[7] "Guinea digitizing telecoms regulation", Connecting Africa, August 2021
[8] "Gateway Internacional Angola ensures secure international calls to telecom operators", Ver Angola, March 2021
[9] "Tanzanian regulator receives control of monitoring system from Global Voice Group", Developing Telecoms, January 2019
[10] "Kelni GVG to upgrade Common Monitoring Platform (CMP) this year", Biztech Africa, February 2021

2 Assessing the impact of TTMS in Sub-Saharan Africa

More than a decade has passed since TTMS platforms debuted in Sub-Saharan Africa to monitor international traffic. Since then, several countries in the region have adopted TTMS platforms or announced plans to do so, while the scope of the platforms has expanded to include more services. GSMA conducted a survey of NRAs and mobile operators across Sub-Saharan Africa to understand the impact of TTMS implementations from the perspective of various stakeholders.

Reasons for implementation

A good place to start is to understand the reasons for the implementation of TTMS platforms from the perspective of governments and NRAs. The most common reasons provided by respondents to the GSMA survey are as follows:

- **SIM box fraud** – To eliminate SIM box fraud and boost revenue from international incoming calls by ensuring that traffic goes through legal routes.
- **Revenue assurance** – To verify telecoms traffic and ascertain all telecoms-related taxes, levies and regulatory fees due to government from the use of telecoms services.
- **Network traffic verification** – To verify telecoms operators' declarations on traffic data and other network activities on the assumption of misreporting by operators.
- **Device monitoring** – To measure the prevalence of grey and blacklisted devices connected to mobile networks in the country and inform policy response.
- **Pricing regulations** – To monitor the pricing of telecoms services to ensure that it aligns with established regulations.
- **Market intelligence** – To gain insights on usage trends and patterns for various telecoms services (e.g. mobile money) and improve stakeholder collaboration and planning.
- **QoS assessment** – To measure the QoS provided by telecoms operators, particularly voice services, against expected standards.
- **Off-net traffic reconciliation** – To reconcile any disputes between telecoms operators relating to the termination of off-net voice calls, and resolve customer complaints on services provided.
- **Big data initiatives** – To build a repository of data from different sectors of the economy, including telecoms, to support overall government big data and smart city initiatives.

- **Staff upskilling** – With technology transfer often built into the contracts for the implementation of TTMS, some national regulators view them as an opportunity to equip staff with new skills.

Impact analysis

Analysis of the impact of TTMS platforms in this study focuses on three areas:

- expectation versus reality of TTMS in preventing SIM box fraud
- the cost-benefit trade-off associated with the implementation of TTMS
- risks to customer data privacy and operator network security.

Note: this research did not find any evidence of telecoms operators misreporting to justify the rationales of revenue assurance and network traffic verification. In Tanzania, for example, network traffic data reported by operators has consistently met the variance limit of 2% set by the TCRA. Furthermore, operators' network data and financial records are subject to rigorous auditing by government and external auditors, which are the appropriate channels to detect and report any misreporting of network traffic data.

SIM box fraud prevention: mismatch between expectation and reality

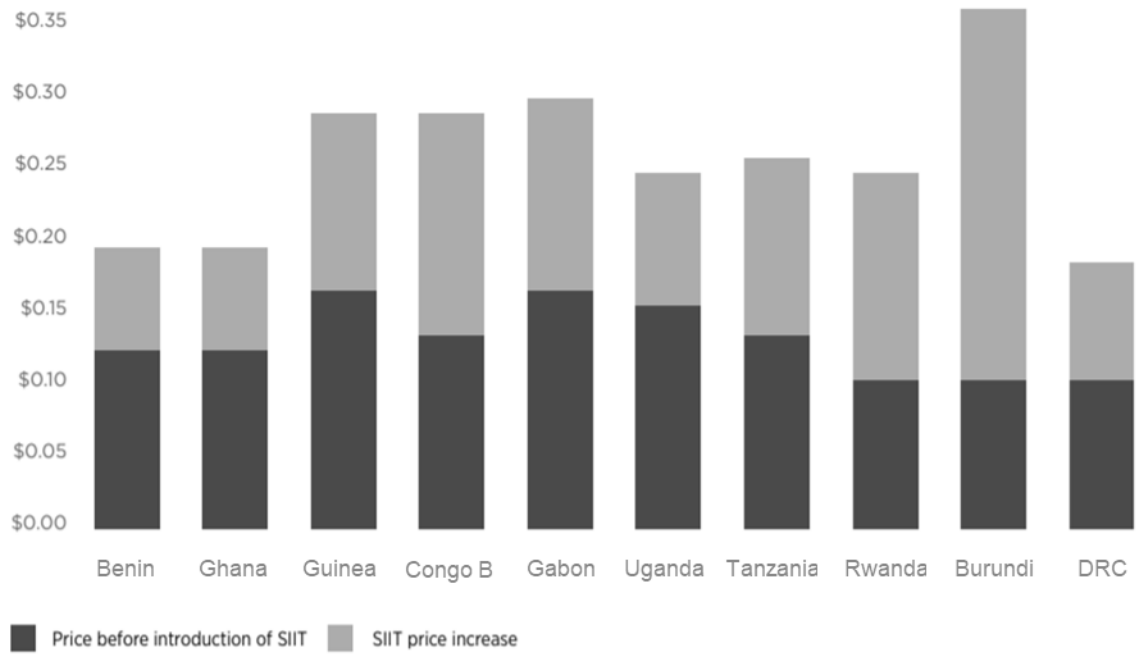
The primary rationale provided by governments and NRAs for the implementation of TTMS platforms was to prevent SIM box fraud, which occurs when fraudsters bypass the voice clearing houses by setting up international calls with low-cost, local prepaid SIM cards. The result has been revenue and tax losses for governments and local operators. There are also security concerns from the manipulation of calling line identification (CLI) during the termination process, which impedes the traceability of such traffic.

The challenge of SIM box fraud is universal. However, it is particularly prevalent in Sub-Saharan Africa, where national regulators estimate that 50–90% of international traffic passed through illegal routes at the peak of this practice.[11] The main driver of SIM box fraud in the region is the incentive for fraudsters to take advantage of the difference in pricing between international and local calls. Meanwhile, the imposition of the surtax on international inbound call termination[12] (SIIT) in some countries further increased the arbitrage opportunity.

Several governments and NRAs implemented TTMS and introduced SIIT during the first half of the last decade. A Deloitte analysis for the GSMA shows that the introduction of SIIT led to a 97%[13] increase in international call tariffs in the affected countries, on average (see Figure 2).

[11] GSMA TTMS survey and key informant interviews
[12] SIIT takes the form of an imposed fixed price that operators must charge for international inbound termination, of which the government takes a set amount
[13] Surtaxes on International Incoming Traffic in Africa, GSMA, 2014

Figure 2: Termination prices for international incoming calls



Source: Deloitte analysis based on data provided by local mobile operators between 2011 and 2013

The expectation was for TTMS platforms to help identify and block grey traffic and, by extension, boost government revenue from SIIT and other related taxes. Indeed, many authorities in the region based their decision to implement TTMS on the promise of increased government revenue from international traffic.

However, research conducted by the OECD noted that the introduction of SIIT in several countries in the region led to a significant decline in international incoming traffic.[14] Evidence presented in the OECD research showed that users made longer calls to countries that had not witnessed significant price increases for termination rates, and that the number of calls received per mobile user in countries with SIIT in place was lower than in countries without SIIT.

Meanwhile, the introduction of SIIT in some countries led to a reciprocal increase in termination rates in neighbouring countries. As a result, local operators reviewed their call tariffs upwards to cushion the impact of additional costs of calls terminating in other countries, resulting in an overall increase in outbound call tariffs for consumers. Recognising the negative impacts of the SIIT on trade and regional integration in the East Africa sub-region, Kenya, Rwanda, Burundi, Uganda and South Sudan agreed in May 2014 to waive the SIIT for calls originating from the sub-region.

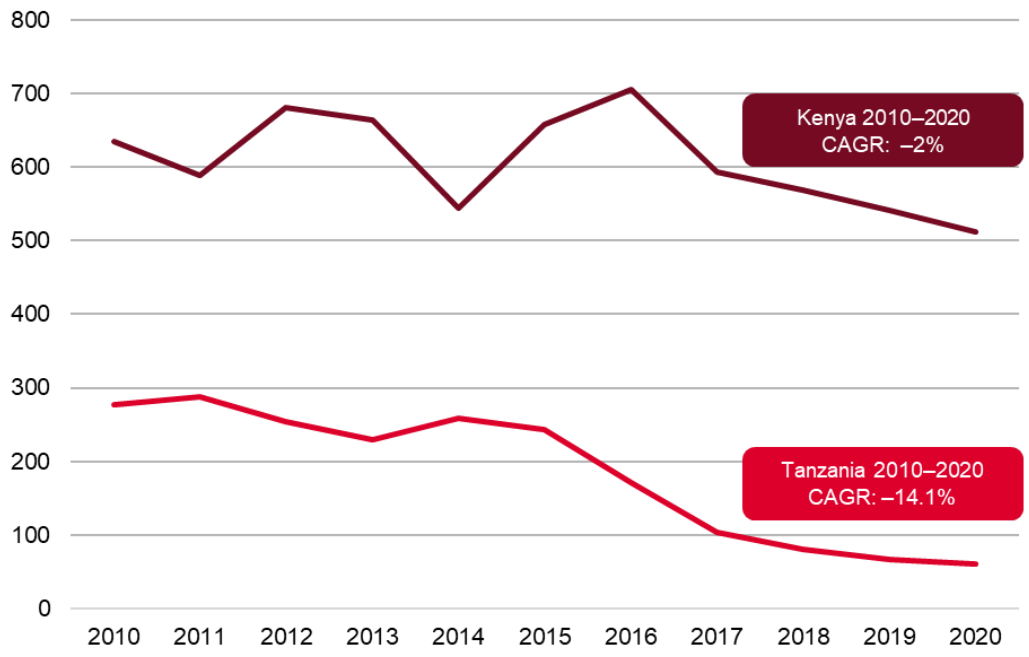
The introduction of TTMS and SIIT coincided with the arrival of popular OTT voice and messaging services, such as Skype, WhatsApp and Viber. These services have had a cannibalising effect on

[14] International Traffic Termination, OECD Digital Economy Papers, No. 238, 2014

local and international voice and messaging services, so the imposition of SIIT (which led to higher international call tariffs) would have exacerbated that impact.

Figure 3 shows the trend in international incoming calls in Tanzania and Kenya between 2010 and 2020 – a period when Tanzania implemented TTMS and SIIT. The annual volume of international incoming calls declined in both countries, largely due to OTT cannibalisation. However, Tanzania witnessed a steeper drop (–14% CAGR) compared to Kenya (–2%), suggesting a more pronounced shift to OTT calling in Tanzania, partly due to higher tariffs.

Figure 3: International incoming calls in Tanzania and Kenya
Million



Source: TCRA, CA, GSMA Intelligence

Similarly, the Republic of the Congo recorded a 36% decrease in incoming international traffic between May 2009 and May 2011, following the introduction of SIIT. An increase in the rate of SIIT in 2017 accelerated the decrease by a further 9%, while operators observed an increase in SIM box activities and OTT traffic over the same period.[15]

While multiple factors have contributed to the decline in international incoming calls and corresponding rise in OTT usage, stakeholders believe that TTMS and SIIT were significant factors, as they accelerated the shift in usage patterns towards cheaper alternatives.

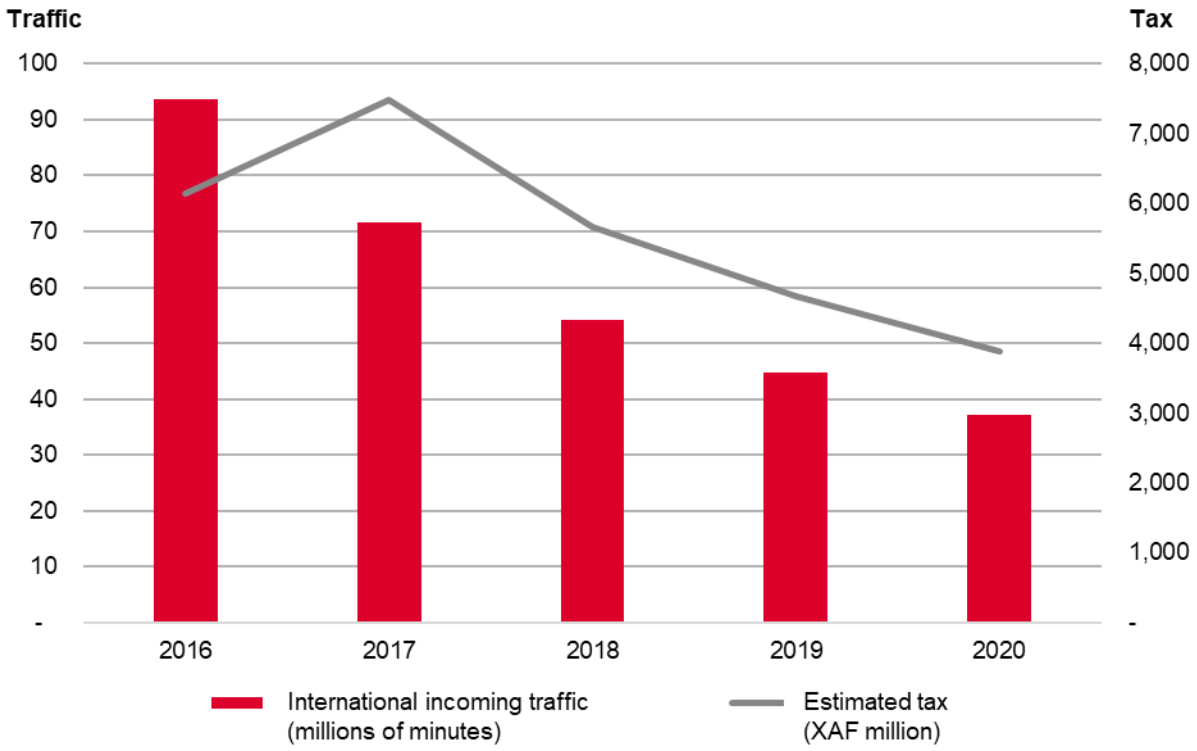
In this regard, the combination of TTMS and SIIT appears to have been counterproductive. High international termination rates have impacted international incoming calls negatively and shattered

[15] GSMA TTMS Survey and key informant interviews

government revenue expectations. As a result, governments have been unable to realise the anticipated revenue uplift upon which the decision to implement TTMS was primarily based.

Figure 4 shows the trend in international incoming calls and tax revenue in the Republic of the Congo between 2016 and 2020, according to a report by the NRA. The value of tax revenue fell by 56% during the period, following a 63% drop in the volume of international incoming calls.

Figure 4: Republic of the Congo: trend in tax revenue* and international incoming call traffic



*Tax on incoming international voice traffic
Source: ARPCE report, January 2022

TTMS platforms, combined with progress that operators are making on fraud management systems, may have played a role in the reduction in SIM box fraud in some countries. For example, Tanzania's TCRA credits the country's TTMS platform for the reduction in grey traffic from 70% of international calls in the early 2010s to just 1% by 2018.[16] However, stakeholders in some other countries believe it may have had the opposite effect, accelerating the activities of fraudsters looking to take advantage of price arbitrage opportunities. Nonetheless, the evidence presented above shows a mismatch between expectations for TTMS and reality.

Meanwhile, the SIIT continues to lead to high monitoring costs to detect fraud. Operators and NRAs actively search for anomalous behaviour in calling patterns to find illegal gateways. The removal of SIIT would alleviate the significant costs and resources devoted by both operators and

[16] GSMA interview with TCRA

authorities to the policing of these illegal gateways. The resources could instead be spent on improving telecoms infrastructure or promoting universal broadband access, for example.

The weakening of the original rationale for TTMS is seen as the main reason for the expansion of the scope of such platforms to include other services, such as data traffic and mobile money. It has also led to the conception of new rationales to justify investment in TTMS platforms. However, the business case for these new rationales is uncertain, given that there is no obvious revenue opportunity, as was the case with efforts to block grey traffic. This has raised concerns about the potential for governments to impose usage taxes on a range of services, such as mobile money, based on transaction data monitored on TTMS platforms.

The cost-benefit trade-off

A key issue for governments and NRAs to consider is whether the cost of deploying and maintaining TTMS platforms is worth the value provided. This should be viewed in the context that these platforms are becoming more resource-intensive as network complexity increases and the number of multi-generational networks (2G/3G/4G/5G) grows. The cost of implementing a TTMS platform depends on a number of factors, such as the scope, functionality and number of subscribers involved. In Ghana, for example, the government agreed a five-year deal worth $89 million in 2017[17] with a third-party supplier. More recently, the Lesotho government agreed to a LSL500 million ($36 million) deal over seven years with the same supplier.[18]

In most cases in Sub-Saharan Africa, TTMS platforms have been financed by governments directly or through build-operate-transfer (BOT)/revenue-sharing financial models with the third-party supplier. Governments and NRAs expected the revenue uplift from blocking grey traffic to fund the TTMS contracts. However, there are cases where authorities have shifted part of or the entire burden to operators, which constitutes an additional tax on mobile services. Examples include the following:

- In the Democratic Republic of Congo (DRC), the NRA is implementing a TTMS platform with funding from the World Bank.[19] This is in addition to a 60% increase in SIIT from $0.05 to $0.08 in 2013 to fund a TTMS platform. Furthermore, a new decree issued in March 2022 provides for the levy of $0.0075 per minute, $0.003 per SMS and $0.00005 per Mb for the management and maintenance of a TTMS platform that is currently being implemented, among other purposes.

- In Lesotho, the authorities have proposed a model based on a levy on mobile operators to fund a TTMS platform.

[17] "Exclusive: Full $89m contract between Ghana and Kelni GVG", StarrFM Online, September 2022
[18] "Minister denies harassment charge", The Post, June 2021
[19] Autorité de Régulation de la Poste et des Télécommunications du Congo (ARPTC)

- In the Republic of the Congo, the NRA paid the initial cost of deploying the TTMS platform, but now transfers 19.3% of the monthly tax paid by the operators to the third-party technical partner as management fees for the platform.

TTMS also informs a number of sector-specific taxes on the telecoms sector, such as excise duty on traffic (voice, data and SMS), interconnect tax levied on off-net traffic and taxes on mobile money services. For example, in 2018, the Liberia Telecommunication Authority (LTA) imposed price floors and surcharges on voice calls and data, putting an end to three-day unlimited calls and data bundles that previously cost $1 and upon which many low-income users relied.[20]

Funding TTMS platforms directly or indirectly from the telecoms sector puts an extra burden on operators and disproportionately affects the most vulnerable users. For example, additional levies can divert investments away from much needed infrastructure and services in underserved areas, while increases in the cost of communication services for end users could erode the significant strides made towards digital inclusion. Essentially, where operators bear part or the entire cost for the initial implementation and/or ongoing maintenance of TTMS platforms, the additional cost burden is ultimately borne by customers through higher costs and poor QoS.

This has the potential to make the fundamental right to communicate and access digital services more challenging for those at the bottom of the socioeconomic pyramid – at a time when consumers in many countries face high inflation and rising costs, and when the growing digital divide between developed and developing regions, highlighted by the pandemic, calls for more investment in infrastructure rollout to underserved areas.

Notwithstanding the source of funding, authorities also need to consider whether the value derived from a TTMS platform justifies the cost of deployment and ongoing maintenance, given other pressing public funding needs. This is especially crucial considering operators have already invested in monitoring tools for networks and can provide the required traffic data. This means that, in reality, TTMS platforms are largely duplicative with nominal additional value, considering the resources spent on their implementation and ongoing maintenance.

Generally, operators provide network traffic data and other statistics to NRAs on a regular (e.g. monthly, quarterly or annually) and ad hoc basis. Indeed, NRAs regularly visit operators on network and operation monitoring exercises, often with live/near-live access to network systems for various reasons.

[20] "In Liberia, a new mobile phone tariff collides with digital rights", Global Voices, July 2020

Data privacy and network security

Fundamentally, TTMS platforms are external to the telecoms network, irrespective of the level of intrusion. In some cases, the platforms connect into the telecoms network through probes; in others, operators are obligated to route traffic through a monitoring gateway. The platforms collect, process and store a huge amount of data, to varying degrees of granularity. Indeed, some platforms in operation in the region are equipped to collect call data records (CDRs), location data and, potentially, other sensitive customer data.

These facts are a source of concern for NRAs and operators alike. Risks highlighted by these stakeholders in the GSMA TTMS survey include the following:

- Technical issues often arise from interconnecting with third-party systems, and resources (time, personnel, etc) are required to resolve such issues. This adds to the workload of already stretched operator staff.

- The telecoms network is vulnerable to cyberattacks, given that the external connection to the network and the associated expanded threat surface presents a point of weakness.

- There is a high risk of violation of customers' data privacy. Operators are obligated by their licensing requirements to maintain the highest standards of customer data protection and security, but the third-party suppliers of the TTMS platforms are often not held to similar standards.

- Because of the rich data they collect, process and store, the TTMS platforms constitute an extremely attractive target for hostile nation states or other malicious actors. Exploitation of vulnerabilities has the potential to significantly undermine national security.

- Some countries have had multiple third-party suppliers and sub-contractors. Little or no government oversight of their data governance practices and track record, particularly in a sensitive sector such as telecoms, could be a potential threat to national security.

- The expansion of the scope of TTMS platforms to cover other services adds to the complexity of the system. The need to connect on so many different nodes within the network creates new challenges for operators.

- From an NRA perspective, the fact that different operators in the market use different network systems poses its own challenges; the TTMS platform may need to be configured to deal with the peculiarities of each network.

In some cases, governments have taken steps to mitigate some of these risks. Examples include mandating that data collected from telecoms networks is processed and stored locally, clearly defining what needs to be measured to avoid scope-creep, and using passive probes to measure traffic in order to avoid interference with the normal functioning of the network. Furthermore, some NRAs highlighted efforts to facilitate collaboration among various parties, particularly operators and

the third-party TTMS supplier, to ensure the smooth implementation and management of the platform.

Protecting national telecoms infrastructure and customer data has become a top priority for governments around the world, given the increasingly integral role that connectivity plays in society. Implementing TTMS platforms and exposing the telecoms network increases the risks of cyberattacks and misuse of customer data.

This is particularly the case in Sub-Saharan Africa, where governments often rely on private, third-party companies to implement and manage TTMS platforms due to a lack of skills and technical capabilities. Governments and NRAs must recognise the security and data privacy risks associated with allowing non-state actors access to sensitive data and national telecoms infrastructure.

3. Best practice for telecoms traffic data monitoring

The telecoms sector plays a pivotal role in society, from enabling access to connectivity and life-enhancing services online to contributing directly to economic growth and social progress. At the same time, telecoms networks generate a huge amount of data that, when anonymised and analysed, can produce useful insights for decision makers. In this context, governments around the world have taken a keen interest in telecoms usage data and the financial returns from the telecoms sector.

However, the sensitivity of telecoms infrastructure and data underlines the need for authorities to adopt the right approach in collecting, processing and storing network data. Some countries in Sub-Saharan Africa have implemented third-party platforms as a means to monitor telecoms traffic data, but the majority have not. The assessment of the impact of TTMS platforms in the previous chapter suggests that the costs and risks associated with implementing a third-party solution in the telecoms infrastructure far outweigh the benefits.

Best practices and alternative approaches to telecoms traffic monitoring

Use more efficient methods for network traffic and revenue verification

Governments should equip relevant agencies with the right skills and tools to carry out revenue assurance duties on behalf of the government. This will ensure the accurate calculation of taxes due to the government, and avoid the need for further audits using TTMS. Meanwhile, the nature of bundled products and customer-specific offers means that operators carefully track their effective rates per minute (i.e. total revenue for a service divided by total traffic minutes), which vary over time depending on the offers in the market. The effective rate per minute multiplied by traffic minutes for the service is a much more accurate estimate of revenue collected. As such, a more nuanced auditing process is required to compute taxes and verify revenues.

Work with operators to fight and curb fraudulent traffic

Operators have a significant interest in curbing grey traffic, given its impact on revenues and QoS. They have invested in technical solutions and systems to detect and prevent revenue leakage, fraud and security issues, which authorities can leverage to achieve their objectives. Best practices around the world are based on cooperation and trust between operators and regulators, as well as information and insight sharing to improve QoS and tackle SIM box fraud. This has proven to be a more effective and less risky way of curbing grey traffic than the use of TTMS. In this regard, NRAs and other government authorities should undertake a study in consultation with operators to establish the veracity of any claims regarding SIM box fraud and revenue leakages and work collaboratively to address such issues.

Work with operators to extract relevant traffic data

Operators are caught between increasing regulatory demands to access data and consumer/enterprise customers' desire for privacy. Where governments need traffic data (e.g. for planning purposes and to gain insights on the digital economy), they should work with operators to agree a feasible mechanism to access this data in line with established data privacy standards. This will help avoid duplication of efforts and other risks associated with the implementation of TTMS for the same purpose.

Protect citizens' data

The use of TTMS platforms from non-state actors presents significant risks to citizens' data, with the potential to impact consumer trust in digital services. Governments must recognise the risk of giving unfettered access to sensitive network data to non-state actors and the implications for national security and customer data privacy. All data and information collected must be treated in compliance with the relevant privacy laws and regulations.

Base decisions on evidence

In countries where revenue assurance and network traffic verification were identified as key to the rationale for the implementation of TTMS, no study has been undertaken to show evidence of misreporting by operators. Claims regarding revenue leakages, without the necessary study or evidence to establish their veracity, are unfounded and unjustified. Furthermore, accusations of misreporting can result in reputational damage for operators and mistrust among stakeholders.

Ensure a level playing field for all sectors

In many instances, the telecoms sector faces more stringent revenue assurance obligations than other sectors of the economy. This approach results in an additional burden on operators.

Avoid expanding the scope of existing systems

Extending TTMS platforms to cover other services poses significant technical and operational challenges for operators, including exposing the network to cyberattacks by weakening the systems established by operators. Furthermore, expanding the scope of traffic monitoring now to include domestic traffic, data traffic and mobile money transactions is seen as a precursor to the imposition of new fees and taxes, as well as per-minute revenue-sharing models for national traffic. These rent-seeking practices place an increased cost burden on operators (which already face disproportionate sector-specific tax burdens) and impact affordability for customers.

Technology, products and services, and customer behaviour have evolved significantly over the last decade, and TTMS platforms no longer achieve their original intent – to monitor incoming international traffic to ensure collection of the SIIT and prevent fraud. Fundamentally, international voice traffic is declining steadily as customers are moving to other technologies such as OTT calls and instant messaging, which are not subject to regulation or SIIT. In this context, authorities should adopt alternative approaches to telecoms traffic monitoring and reassess the value of TTMS platforms, where they exist, against the associated costs and risks. Furthermore, there is a need for constant engagement between authorities and operators to facilitate information sharing and ensure that the highest standards of data privacy and network security are met.

Appendix

Research methodology

This report utilised secondary research and data from GSMA Intelligence and primary data and insights from a survey of mobile operators and regulators across Sub-Saharan Africa. Interviews and questionnaire responses were from: two operator groups, representing 20 operators across the region; four other single network operators; one national industry association; and seven regulators.

Glossary

Defining Sub-Saharan Africa

Angola, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroon, Chad, Congo, Côte d'Ivoire, DRC, Ethiopia, Gabon, Gambia, Ghana, Guinea, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Rwanda, Senegal, Sierra Leone, South Africa, Swaziland, Tanzania, Togo, Uganda, Zambia and Zimbabwe.

Terms and abbreviations

- ARCEP Niger – Regulatory Authority for Electronic Communications and Post of Niger
- ARPCE Congo – Postal and Electronic Communications Regulatory Agency of Congo
- CDR – call detail record – information generated by telephone exchanges or any other telecoms equipment including data on calls originating from, terminating at, or passing through the exchange or equipment, and call duration
- CLI – calling line identification
- Gateway – switching system through which telecoms traffic is interchanged (interconnection) between local telecoms operators and international carriers, with provisions for allowing physical monitoring of traffic flow
- Grey traffic – international traffic that is illegally exchanged between the local licensed telecoms operators and foreign operators operating from outside from the country, bypassing the legal routes and exchanges
- International incoming telecoms traffic – traffic originating from outside the local operator and terminating in the local operator, either to a public switched telephone network (PSTN), public land mobile network operator, internet access provider, unified telecoms service operator, network facilities operator, network service operator, international gateway services operator or application service provider

- International outgoing telecoms traffic – traffic originating from the local country and terminating in any country outside the given country, from a telecoms licence holder

- Monitoring – observation and supervision of telecoms traffic, in particular, signalling data, excluding the capability to record, monitor or tap into the content of any personal communication

- National interconnection traffic – traffic exchanged between local operators (off-net) and traffic within the network of telecoms licensees (on-net)

- SIIT – surtax on international incoming traffic

- TCRA – Tanzania Communications Regulatory Authority

- Telecoms traffic – the amount of data, volume of voice or number of messages carried over a communication channel in a given period

- TTMS – telecoms traffic monitoring system

GSMA™

GSMA Head Office
1 Angel Lane,
London, EC4R 3AB
United Kingdom

Tel: +44 (0) 20 7356 0600
Fax: +44 (0) 20 7356 0601