Safaricom And Internet Traffic Tampering

CIPIT Research Brief
Nairobi, March 2017

CIPIT
CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

Summary

Technical research conducted on several Internet service providers in Kenya for the last ten months between June 2016 and March 2017 indicates the presence of a middle-box on the cellular network of one provider, Safaricom Limited.

Middle-boxes assume dual-use character in that they can be used for legitimate functions (e.g., network optimisation) while simultaneously being used for traffic manipulation, surveillance and aiding censorship.

In light of such dual uses, this report makes clear that service providers operating middle-boxes must communicate to the public in a transparent manner the justification for such activity. This is especially relevant as government bodies announce plans to monitor the Internet during Kenya's current electoral processes.

Introduction

CIPIT has been conducting network measurements on Kenyan Internet Service Providers (ISPs) since June 2016 using assorted techniques. Between 6 - 10 February 2017, the data indicated the presence of a middle-box on Safaricom's network (AS33771) that had not previously presented any signs of traffic manipulation.

Shortly after reaching out to the company for further information on these observations, a technical team from the company denied the presence of a middle-box in their data. Within a few days, however, we noticed the tests once again returning negative activity for a middle-box (i.e., we did not observe further middle-box activity) .

We have not, to date, received official communication from Safaricom Limited on our findings. This brief will present the methodology we use to detect middle-boxes, then illustrate how that methodology was applied on Safaricom's network, as well as our findings from such investigations.

Finally, we present a contextualization of these findings within the political and legal processes in Kenya.

How do we detect middle-boxes?[1]

The HTTP Invalid Request Line test by the Open Observatory of Network Monitoring (OONI) tries to detect the presence of censorship and/or surveillance software ("middle-box") which could be responsible for traffic manipulation.

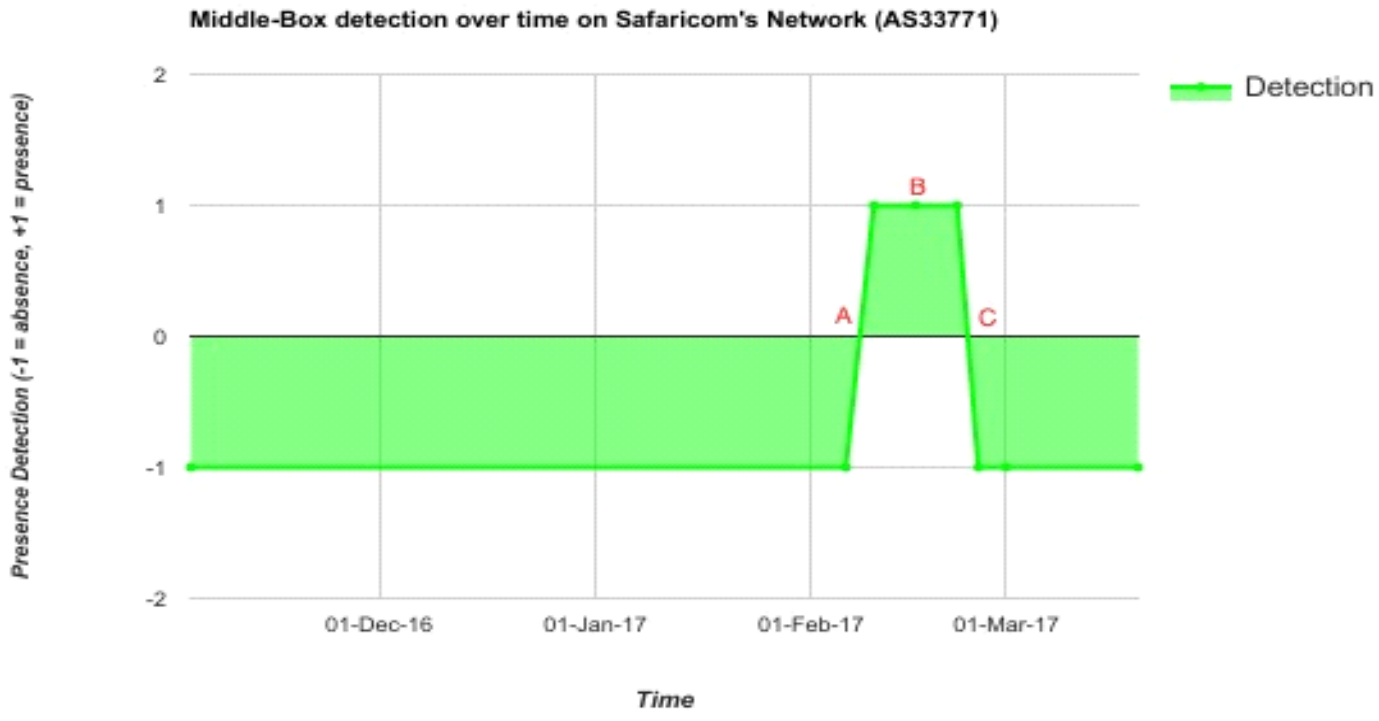
Instead of sending a normal HTTP request, the client sends an invalid HTTP request line - containing an invalid HTTP version number, an invalid field count and a huge request method – to an echo service listening on the standard HTTP port. If a middle-box is not present in the network between the user and an echo service, then the echo service will send the invalid HTTP request line back to the user, exactly as it received it. In such cases, it is assumed that there is no visible traffic manipulation in the tested network.

If, however, a middle box is present in the tested network, the invalid HTTP request line will be intercepted by the middle box and this may trigger an error and that will subsequently be sent back to OONI. Such errors indicate that software for traffic manipulation is likely placed in the tested network, though it's not always clear what that software is. In some cases though, we are able to identify censorship and/or surveillance vendors through the error messages in the received invalid HTTP responses.
So far, using this technique, OONI and its partners have detected *BlueCoat, Squid and Privoxy* in networks across 11 countries around the world.

1. For more on this, see HTTP Requests https://ooni.torproject.org/nettest/http-requests/

A false negative could potentially occur in the hypothetical instance that ISPs are using highly sophisticated censorship and/or surveillance software that is specifically designed to not trigger errors when receiving invalid HTTP request lines like the ones of this test. Furthermore, the presence of a middle box is not necessarily indicative of traffic manipulation, as they are often used in networks for caching purposes.

Middle-Box Detection on Safaricom Network (AS33771)



The figure above visualizes the detection of middle-box on Safaricom's network (point A), notification (B), engagement and its disappearance (C) between November 2016 and March 2017. For the raw data, please see Annex 1

Manipulation Detected

On 10 February 2017, our measurements showed signs of traffic manipulation, a sign of a middle-box presence based on OONI's methodology. As illustrated in the data collected from 10 February 2017 (provided as Annex 1 to this report), the HTTP responses received were different from what had originally been sent. This traffic manipulation persisted through end of February to early March 2017.

Responsible Disclosure

After detecting this traffic anomaly, we contacted Safaricom Limited requesting confirmation on the presence of a middle-box and, if necessary, justification for such activity. .
On 24 February 2017, Safaricom, through a conference call, put us in touch with the subject matter technical team who sought to know the rationale of such research and further details regarding the technical background of the HTTP Invalid Request Line test. The technical team denied the presence of any middle-box in their networks and promised a more detailed response in five days. By the time of this publication, 15 days later, we had not received any communication from the network, despite our reminders.

Tampering Signs Disappear

On 27 February 2017, two days after our contact with Safaricom's technical team, tests conducted on the network showed the absence of network tampering. As shown by the data attached in Annex 1, the invalid HTTP requests sent over Safaricom's network are returned back exactly as they were sent, indicating the absence of a middle-box.

This apparent change implies two possibilities; the probable middle-box was reconfigured to avoid triggering errors from the invalid http requests, or that the network dropped the probable middle-box in the network. Either way, the silence from Safaricom to respond to our request in a conclusive way raises more questions than answers from the leading communication provider in Kenya.

Kenyan Government's Intent to Monitor Social Media

On January 2017, Kenya's official communication sector regulator, the Communication Authority (CA), announced plans to monitor social media during the 2017 General Elections process in partnership with the Criminal Investigation Department of the Kenya Police[2]

The CA has also announced plans to install a device management system on all telecommunication companies in Kenya to weed out counterfeit devices from operation. This is directed towards telephone calls and not the Internet services, according to the tender document specifications.[3]

The device management system deployment has been challenged in court and effectively suspended to allow for hearing.[4]Telecommunication companies, Safaricom included, have displayed significant opposition to the CA requirement citing privacy guaranteed of their subscribers communication.

The National Cohesion and Integration Commission (NCIC), a body meant to monitor hate speech and promote integration has also announced plans to actively monitor social media and flag users who incite hatred during the electoral process.[5]

Kenya has a history of Internet mass surveillance as illustrated by, among others, Wikileaks dumps, Edward Snowden leaks, Citizen Lab reports, and Privacy International findings. This has for the most part been justified under counter-terrorism grounds and executed through nation-state partnerships.

For this to work, privately owned Internet service providers aid in the execution of mass surveillance and in the absence of transparency on such processes, they cannot guarantee the integrity of communication on their platforms for citizens.

2. Gicobi, M. (2017). Kenya to monitor social media during elections. The EastAfrican. [online] Available at: http://www.theeastafrican.co.ke/news/Kenya-to-monitor-social-media-during-elections/2558-3515588-cwdl3i/index.html [Accessed 14 Mar. 2017].
3. IFMIS (2016) Design, Supply, Delivery, Installation, Testing, Commissioning and Maintenance of a Device Management System (DMS)
4. The Nation, (2017). Court stops communications agency from phone tapping. [online] Available at: http://www.nation.co.ke/news/1056-3821000-3bnjlfz/ [Accessed 14 Mar. 2017].
5. Ruto, P. (2016). 'Hate' body to monitor social media ahead of polls. The Nation. [online] Available at: https://citizentv.co.ke/news/hate-body-to-monitor-social-media-ahead-of-polls-151441/ [Accessed 14 Mar. 2017].

Privacy, Internet Intermediaries and the Kenyan Law

The Kenyan Constitution (2010) under Articles 31(c) and (d) provides for the right of every person not to have "information relating to their family or private affairs unnecessarily required or revealed" and "the privacy of their communications infringed".[6] This can however be suspended during a gazetted state of emergency as provided for under Article 58 of the constitution.[7]

The country has not yet enacted a law to this section of the constitution, with the data protection bill still in draft format six years after initial drafts.Even without a Data Protection Law in, there does exist a host of legal instruments to guide the practice of data collection, processing and sharing.

In reference to communication intermediaries, the Kenya Information and Communication Act (2010) under section 31 provides for the prosecution of telecommunication providers if:

> *"otherwise than in the course of [their] business -- (a) intercepts a message sent through a licensed telecommunication system; or (b) discloses to any person the contents of a message intercepted under paragraph (a); or (c) discloses to any person the contents of any statement or account specifying the telecommunication services provided by means of that statement or account".*

Further, the Kenya Information and Communications (Consumer Protection) Regulations (2010), states that a licensee:

> *"shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data".*

6. Kenya Constitution 2010, http://kenyalaw.org/kl/index.php?id=398
7. See Part 4 of the Bill of Rights: State of Emergency, Article 58 (6) a

Kenya is also party to several international treaties and conventions that require the country to abide to privacy rights. These, among others, include the African Union Principles on Freedom of Expression, the Universal Declaration on Human Rights, and the International Convention on Civil and Political Rights.

Some legal developments in the last five years have created avenues for suspending privacy expectations as set out in the constitution. In 2014, the Communication Authority published the *Registration of Subscribers of Telecommunication Services Regulations* which require a licensee (telecommunication companies operating in Kenya) to permit the Regulator access to its systems, premises, facilities, files, records and other data to enable the Commission inspect such systems, premises, facilities, files, records and other data for compliance with the Act and these Regulations.[8]

The *Security Laws (Amendment) Act (2014)* provide for National Security Organs to intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary. Article 69 (3) provides:

> *"The right to privacy under Article 31 of the Constitution shall be limited under this section for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism."*

The Communication Authority, the communication sector regulator, has pronounced itself on possible scenarios of Internet censorship and or surveillance as explained in the section above. if 'things get out hand' is one such scenario where complete censorship (Internet shutdown) can be activated.[9] Before that, procurement for social media surveillance has already been made in preparedness for elections.[10] These early signs before the August 8 elections point to the need for a proactive privacy conscious policy engagement in Kenya.

Conclusions and Recommendations.

Our open methodology of detecting presence of middle-boxes on a network confirms that out of the five networks tested in the last ten months in Kenya, only one has a middle-box. After contacting the network that showed signs of network tampering, the technical team denied of any middle-box but soon afterwards, our tests stopped detecting the middle-box. We conclude that the middle-box was configured to avoid triggering errors from the invalid http requests, or that the network dropped the probable middle-box in the network.

The role of Internet service providers in defending against human rights violations on the Internet cannot be overemphasized. To the extent possible, companies should maintain a transparency policy on privacy protections or violations using existing legal structures. The silence from Safaricom to respond to our request in a conclusive way raises more questions than answers from the leading communication provider in Kenya.

The Data Protection Bill 2013, which is meant to give life to Article 31 of the Constitution, should be prioritized to ensure the deployment of data collection infrastructure in the country has the requisite safeguards.

The judiciary plays a significant role on the interpretation of domestic and International legal instruments on privacy and telecommunications. Continuous legal training of the judiciary officials should increasingly incorporate new developments in the technical fields, in this case, for example, the deployment of dual-use technologies and its implications on privacy.

8. Kenya Law, 2014, http://kenyalaw.org/kl/index.php?id=4215#jfmulticontent_c10756-13
9. http://www.iafrikan.com/2017/01/14/the-kenyan-government-will-only-shut-down-the-internet-during-elections-if-things-get-out-of-hand/
10. Ibid.

Acknowledgments

Ford Foundation for funding the '*Information Controls and Electoral Processes in Kenya'* project.

Open Observatory of Network Interference *(OONI)* for our continued partnership on Internet censorship and surveillance research.

Many others involved in the project who have sought anonymity.

Annex 1

Raw Data on Detecting Middle-Boxes on Kenyan Internet Service Providers

Sections

Safaricom (AS33771)
- No Manipulation Detected (Baseline data)
- Manipulation Detected
- Responsible Disclosure
- Tampering Signs Disappear

Jamii Telkom Limited - Faiba (AS36866)
- No Tampering Detected

Wananchi - Zuku (AS15399)
- No Tampering Detected

Telkom Kenya - Orange (AS12455)
- No Tampering Detected

Airtel Kenya - Airtel (AS36926)
- No Tampering Detected

The data below shows the responses we got on various networks in Kenya. For more data, please visit Kenya's page on the Open Observatory of Network Interference (OONI's) explorer: https://explorer.ooni.torproject.org/country/KE
The study covered Safaricom, Zuku, Jamii, Airtel and Orange Kenya.

Safaricom (AS33771)

No Manipulation Detected (Baseline data)

Traffic manipulation not detected - November 4 2016
https://explorer.ooni.torproject.org/measurement/20161104T090302Z_AS33771_cWTkafpu8SaTjTXSVKebwUHCp8ekQVyFqv1f1iua3nvN9XaTk9

Traffic manipulation not detected - February 6 2017
https://explorer.ooni.torproject.org/measurement/20170206T003852Z_AS33771_lu-6vCFdzp2l3DVgJZrqCX4UgsDufPqTgQL0PD8dii6sxgkS7kC

Manipulation Detected

Traffic Manipulation Detected - February 10 2017
https://explorer.ooni.torproject.org/measurement/20170210T143704Z_AS33771_YVB017u1RcJt93h7cKGo9zTo5YkgxdW6ORFOHide6K536PhEA5?input=

Traffic Manipulation Detected - February 16 2017
https://explorer.ooni.torproject.org/measurement/20170216T190534Z_AS33771_Y7UaEVg0pQyU7g2lAwkcY5CP0AXCHwekFXg8DGOxoJtsqrXR6S?input=

0654 / HTTP/1.1 | 0654 / HTTP/1.1

SRHY2R1XS4J3WXIGFHC819SENWTARJKRURT2L6OK96MA4T2EWC52V1C875TJX5N46PGJMVJEVU5UIDC-G1IH0G0U7JUUQ6VAP0YB2LBQ56PWWCXNOU2Q3NMTYVAYAGSWBF28JIZFTDY746UXRBJ3CGSJH2IZWY-QF03GCRWJ4LYGQVHK0DB55RYORGDK1AQSA8OG2JFCQI17EZB6RUY062TYLA2YXN4JNJH96WWED-PAF28TDZ94ADY43P2NGPRB26QSF8XUX6MU7AC29IUSAB251JKSL1KF7YITM3IHZMSASFRC65YDOW75XD-FZIQ6ZUH9XI23JPL5XUWJI3MWUIX50FJ28HWD1LW0VIK6FFV6G3CTD7KMX4DYMK33BE3GNJIZD5DMVJSY-F7644GEQ0OD1UXY62TOLTASHEPO3U80FTFEPDS9TMJJI1CVD243ARTLVDSF8TP697ZLZ8OZ8LEJJUFZ9D-JSCXFS76ZPXG83EWLCFGKBI07KIIPOTEUTCSZKW5EGNTDQTAWU6D7KYOW3Q4CIU4E47GZJT63VBND-KXF0FZZQQGETHNM8K59OLB8V05QKV4MLEU2D63Z6EWSJBAVYGAK7LD6Q1E6TWWJT5IHSJ2GDI3ITL0T-1LABD7R7TL1ZF8BOTPTWKLKVQFB3X0AUPT9ID7UJZD9WSHEPGF6VG67QJX810JI4WLWH3YZW83XR-91R4VVO7EYFATW4OQRFAVMVSHMZOMYGFKVSB24P1H7JSGI7Q6YFNDGRF0DQZCIE4VXJ8E9Q7558X-VO61X53BDMH5R5YUFLVR57622DOND9AIT40RN6W00TEMVF7LI7KA8697380ABZWB2B9EOPD248HRI0G-G66Y5D7C5BUOYAKV5LN9CZWZI01FJ2K8C2CI4ECU0Z87935C54PNK3HUI3N2HQSY54OEODZ3L8UXQPO-ICXRPKB8KJGKLDJ7TOCGFRCGKYS28THLRJLIEB4AIC9VT9IRJZEY3B91YT2724C014ZSP1J6RJ303HCE6RS09/ HTTP/1.1

SRHY2R1XS4J3WXIGFHC819SENWTARJKRURT2L6OK96MA4T2EWC52V1C875TJX5N46PGJMVJEVU5UIDC-G1IH0G0U7JUUQ6VAP0YB2LBQ56PWWCXNOU2Q3NMTYVAYAGSWBF28JIZFTDY746UXRBJ3CGSJH2IZWY-QF03GCRWJ4LYGQVHK0DB55RYORGDK1AQSA8OG2JFCQI17EZB6RUY062TYLA2YXN4JNJH96WWED-PAF28TDZ94ADY43P2NGPRB26QSF8XUX6MU7AC29IUSAB251JKSL1KF7YITM3IHZMSASFRC65YDOW75XD-FZIQ6ZUH9XI23JPL5XUWJI3MWUIX50FJ28HWD1LW0VIK6FFV6G3CTD7KMX4DYMK33BE3GNJIZD5DMVJSY-F7644GEQ0OD1UXY62TOLTASHEPO3U80FTFEPDS9TMJJI1CVD243ARTLVDSF8TP697ZLZ8OZ8LEJJUFZ9D-JSCXFS76ZPXG83EWLCFGKBI07KIIPOTEUTCSZKW5EGNTDQTAWU6D7KYOW3Q4CIU4E47GZJT63VBND-KXF0FZZQQGETHNM8K59OLB8V05QKV4MLEU2D63Z6EWSJBAVYGAK7LD6Q1E6TWWJT5IHSJ2GDI3ITL0T-1LABD7R7TL1ZF8BOTPTWKLKVQFB3X0AUPT9ID7UJZD9WSHEPGF6VG67QJX810JI4WLWH3YZW83XR-91R4VVO7EYFATW4OQRFAVMVSHMZOMYGFKVSB24P1H7JSGI7Q6YFNDGRF0DQZCIE4VXJ8E9Q7558X-VO61X53BDMH5R5YUFLVR57622DOND9AIT40RN6W00TEMVF7LI7KA8697380ABZWB2B9EOPD248HRI0G-G66Y5D7C5BUOYAKV5LN9CZWZI01FJ2K8C2CI4ECU0Z87935C54PNK3HUI3N2HQSY54OEODZ3L8UXQPO-ICXRPKB8KJGKLDJ7TOCGFRCGKYS28THLRJLIEB4AIC9VT9IRJZEY3B91YT2724C014ZSP1J6RJ303HCE6RS09/ HTTP/1.1

GET / HTTP/IE0 | ""

UG5NJ QRLBF J86TD VUNG6 | UG5NJ QRLBF J86TD VUNG6

February 22 2017

Traffic Manipulation still being observed:

https://explorer.ooni.torproject.org/measurement/20170222T222322Z_AS33771_K8rE48JZnWgDJUmA3hxAXBcty7monLBa5rTTEJUhoyVAKLqnAJ?input=

Responsible Disclosure

After detecting this traffic anomaly, we contacted Safaricom Limited requesting confirmation on the presence of a middle-box and, if necessary, justification for such activity. .
On 24 February 2017, Safaricom, through a conference call, put us in touch with the subject matter technical team who sought to know the rationale of such research and further details regarding the technical background of the HTTP Invalid Request Line test. The technical team denied the presence of any middle-box in their networks and promised a more detailed response in five days. By the time of this publication, 15 days later, we had not received any communication from the network, despite our reminders.

Tampering Signs Disappear

On 27 February 2017, two days after our contact with Safaricom's technical team, tests conducted on the network showed the absence of network tampering. As shown by the data attached in Annex 2, the invalid HTTP requests sent over Safaricom's network are returned back exactly as they were sent, indicating the absence of a middle-box.

Jamii Telkom Limited - Faiba (AS36866)

No Tampering Detected

No tampering detected - 06 September 2016
https://explorer.ooni.torproject.org/measurement/20170319T090640Z_AS36866_95mrUuBcoWQ7MjB53KrRkPwi9KeNs71OWum9WrojMYopT58sXC?input=

No tampering detected - 16 September 2016
https://explorer.ooni.torproject.org/measurement/20160916T083517Z_AS36866_qCxSUtYEMfvAbuVSRRZafVcamwihBrNJ6DF1pWb7an9fwWl59L

No tampering detected - 14 December 2016
https://explorer.ooni.torproject.org/measurement/20161214T170034Z_AS36866_Ux-qqEUIhOrWqPOVQ5qo8IUOYtBpdwvgPoydJVQMidDcry869mm

Wananchi - Zuku (AS15399)

No Tampering Detected

No tampering detected - 06 June 2016
https://explorer.ooni.torproject.org/measurement/20160606T192259Z_AS15399_cU9zYUqkzqvaVKCKWeDZNtmXXy4GGwBVvZv0AFXdOZtVOw-FTVA

No tampering detected - 08 October 2016
https://explorer.ooni.torproject.org/measurement/20161008T141357Z_AS15399_xT-pSjKSLdfqF9kOSkD2BhjuW4dbsHbePUa7Y4paklv25SM8mUF

Telkom Kenya - Orange (AS12455)

No Tampering Detected

No tampering detected - 24 February 2017
https://explorer.ooni.torproject.org/measurement/20170224T103211Z_AS12455_9rVC56xFHybXg4ghAceiPc19BI6Kalzdt3SV3z1vJAIKeL5lmC?input=

No tampering detected - 27 February 2017
https://explorer.ooni.torproject.org/measurement/20170227T062843Z_AS12455_1FMVbxlPjP9wRM0KUm0Y0g3eT3tqGAk6f0tFoXrc6pZGIek7pE?input=

Airtel Kenya - Airtel (AS36926)

No Tampering Detected

No tampering detected - 20 February 2017
https://explorer.ooni.torproject.org/measurement/20170220T170149Z_AS36926_P2uX2xAqAlYA0HFSK1WUGvsh0zl06rQdbyEVaHZmY12IG2ytXj?input=

No tampering detected - 09 March 2017
https://explorer.ooni.torproject.org/measurement/20170309T170034Z_AS36926_u5dAOAfkc1JKWy8l1ocXc9Mnq4wFpoEj9X3Xyf40SvWzB7HO79?input=

Annex 2

Our Official Letter to Safaricom Limited

CIPIT
CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

Strathmore University
Law School

Our ref: R01/02/2017

20 February 2017

Director, Corporate Affairs,
Safaricom Limited,
P.O Box 66827, 00800 Nairobi, Kenya.
Tel: +254 722 003272

RE: Evidence of Network Tampering on Safaricom Network (AS33771)

The Centre for Intellectual Property and Information Technology Law (CIPIT) is a research center at Strathmore Law School and carries out research on Internet policy in the African region.

Our recent research indicates the presence of a 'middle box' on Safaricom's network. From our longitudinal data, it suggests traffic manipulation started on the week of February 6 - 10, 2017. Our network probe software is open source, including the results it generates and can be accessed from: https://explorer.ooni.torproject.org/country/KE

We would like to hear your comments on our findings especially as a response to these four questions:

1. Can you confirm that you have indeed deployed a traffic manipulation system, as described above and identified by the probe, on your network?
2. If your answer in Q1 is in the affirmative, kindly indicate your justification for this deployment.
3. Again if your answer to Q1 is in the affirmative, kindly comment on whether such deployment is consistent with relevant statutes, and whether the deployment is authorized under a specific statute?
4. In reference to you transparency reporting, when and where was this information reported to the public?

We would appreciate your response in the next five (5) working days to allow us give a better analysis of our work before publication.

CIPIT, Strathmore Law School

CIPIT
Strathmore Law School
PO Box 59857-00200
Nairobi, Kenya

CIPIT@strathmore.edu
www.cipit.org

Mobile: (254-0719) 690510
Tel: (254-0703) 034612
Fax: (254-20) 6007498

CIPIT

CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW

About CIPIT

The Centre for Intellectual Property and Information Technology Law (CIPIT) is an evidence-based research and training centre based at Strathmore University Law School, Nairobi, Kenya. Our Mission is to study, create, and share knowledge on the development of intellectual property and information technology, especially as they contribute to African Law and Human Rights. We are based at Strathmore University Law School, Nairobi, Kenya.

Our team is multidisciplinary, drawn from law, political science, computer science and development while using diverse methodological approaches to inform debates on ICT applications and regulation.

More about our work can be found on www.cipit.org