PRIVACY INTERNATIONAL

Track, Capture, Kill:

Inside Communications Surveillance and Counterterrorism in Kenya



Track, Capture, Kill:

Inside Communications Surveillance and Counterterrorism in Kenya

March 2017

PRIVACY INTERNATIONAL

www.privacyinternational.org

Acknowledgements

Privacy International acknowledges the many individuals and organisations with whom we spoke who cannot be named.

This report is primarily based on interviews conducted by Privacy International and documentation provided in confidence to Privacy International.

Privacy International is solely responsible for the content of this report.

Contents

Acronyms	5
Executive Summary	6
Introduction	7
Background	8
Extended Powers: But short on Detail	11
Spying First, then 'making it proper'	16
On Your Marks: Infiltrating Telecommunications Networks	19
Getting Ready: Sharing Intel and Preparing Ops	24
Closing in: Surveillance in Kill or Capture Operations	26
Elections and Accountability	32
Recommendations	36
Annex 1: Response from Safaricom	38

Acronyms

AP	Administration Police
ATPU	Anti-Terrorism Police Unit
BTS	Base Transceiver Station
CA/CCK	Communications Authority, formerly Communications Commission of Kenya
CDR	Call Data Record
CID/DCI	Directorate of Criminal Investigations
DMI	Directorate of Military Intelligence, Kenya Defence Forces
GSU	General Services Unit, a paramilitary force officially under the Kenya Police Service Control
IMSI	International Mobile Subscriber Identity
IPOA	Independent Policing Oversight Authority
KDF	Kenya Defence Forces
NCIC	National Cohesion and Integration Comission
NIS/NSIS	National Intelligence Service, formerly National Security Intelligence Service
NPS	National Police Service
Recce	Reconnaissance company, of GSU; aka GSU-Recce aka Recce squad

Executive Summary

This investigation focuses on the techniques, tools and culture of Kenyan police and intelligence agencies' communications surveillance practices. It focuses primarily on the use of surveillance for counterterrorism operations. It contrasts the fiction and reality of how communications content and data is intercepted and how communications data is fed into the cycle of arrests, torture and disappearances.

Communications surveillance is being carried out by Kenyan state actors, essentially without oversight, outside of the procedures required by Kenyan laws. Intercepted communications content and data are used to facilitate gross human rights abuses, to spy on, profile, locate, track – and ultimately arrest, torture, kill or disappear suspects, as this report documents. The Kenyan constitution guarantees freedom from torture, cruel, inhuman and degrading treatment and the right to a fair trial as fundamental rights.

These abuses have marred Kenya's counterterrorism operations and further eroded Kenyans' already weak trust in the agencies responsible for protecting them. This investigation also explores the potential impact of unaccountable communications surveillance on the upcoming 2017 election cycle.

The National Intelligence Service (NIS) regularly shares information with police agencies, some of whom have been engaged in gross human rights abuses, according to multiple independent media, civil society and Kenya National Commission on Human Rights (KNHCR) investigations. The NIS appears to have direct access to communication networks across Kenya. This direct access means that the network operator itself has little to no knowledge of the interception of communications occurring on its network, and therefore no real ability to check these powers or report potentially abusive use of communications surveillance powers. The role of the Communications Authority in facilitating direct access in Kenya requires more scrutiny. All responses to Privacy International's requests for comment are included in the text.

Particularly in an election year, there is a pressing need to begin to reform the practice of communications surveillance, preventing a future threat of greater abuse.

Full recommendations are included at the end of the report.

Introduction

This investigation focuses on the techniques, tools and culture of Kenyan police and intelligence agencies' communications surveillance practices. It focuses primarily on the use of surveillance for counterterrorism operations.[1] It contrasts the fiction and reality of how communications content and data is intercepted, how individuals are tracked and targeted, and how this information is fed into the cycle of arrests, torture and disappearances. Communications surveillance is being carried out by Kenyan state actors, effectively without oversight, outside of the procedures required by Kenyan laws. Information gained by communications surveillance directly facilitates the commission of further grave human rights abuses in Kenya's counterterrorism efforts, including torture and extrajudicial killings.

These abuses have marred Kenya's counterterrorism operations and further eroded Kenyans' already weak trust in the agencies responsible for protecting them. This investigation also explores the potential impact of unaccountable communications surveillance on the upcoming 2017 election cycle.

This investigation is based on interviews carried out and documents acquired by Privacy International in 2016. Privacy International interviewed and/or reviewed testimony of 57 individuals for this investigation, and two forthcoming investigations. Of these, 32 were law enforcement, military or intelligence officers either currently serving or who recently left the service. The remaining interviewees included prosecution and defense lawyers, telecommunications network operator employees, Communication Authority staff, security professionals, and families of disappeared Kenyans.[2]

1 Communications surveillance technology appears to be procured and deployed by Kenyan agencies primarily for the investigation of terrorism. Though political actors, journalists, activists and other citizens are almost certainly spied on by Kenya's law enforcement and intelligence agencies using surveillance technologies, evidence of such practices to date is anecdotal and difficult to disentangle from the less costly and more ubiquitous use of human intelligence networks. Nevertheless, the Kenyan government's desire to use surveillance tools against domestic critics is evident from the National Intelligence Service's attempted procurement of the Remote Control System surveillance product of Italian company Hacking Team in 2015. As a "proof of concept", an NIS agent requested that the Hacking Team take down a website critical of the Kenyan government. The Kenyan government is also alleged to have acquired intrusion malware from FinFisher. See: "WikiLeaks: NIS purchased software to crack websites," The Daily Nation, 11 July 2015, http://www.nation.co.ke/news/NIS-WikiLeaks-Hacking-Team-Surveillance/1056-2784358-2pn97rz/index.html and "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," The Citizen Lab, 15 October 2015, https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

2 Privacy International accepted the request for anonymity of most sources, particularly acting law enforcement and intelligence officers, who would face serious repercussions if identified. Privacy International independently corroborated all sources' identities. No compensation for interviews was provided.

Background

From the intelligence units deployed under British colonial authority to former President Daniel Moi's fearsome spies, Kenya has long had a robust intelligence service. More recently, the Kenyan government's ability to monitor citizens' communications has evolved in response to two dynamics.

The first dynamic is the legacy of sectarian violence following the 2007 election. Over 1,000 Kenyans died in two months of violence among Kenya's major ethnic groups. In 2008, the government created the National Cohesion and Integration Commission (NCIC) to investigate ethnic hate speech complaints. This included increasing scrutiny of communications online and transmitted by SMS. The NCIC teamed up with the then-Communications Commission of Kenya (CCK)[3] to closely monitor online speech.[4] In the run up to the 2012 elections, the CCK issued new regulations to prevent the circulation of inflammatory material.[5] Following the elections, the CCK requested that mobile providers block text messages by firewall using pre-identified key words. The National Steering Committee on Media Monitoring of the Ministry of ICT reportedly intercepted 300,000 SMS messages daily.[6]

The threat of terrorism is the second and more significant pressure that the government cites to justify stricter regulations on speech and closer surveillance of Kenyans' communications. Kenya has experienced dozens of terrorist attacks mainly in Nairobi, and the Coastal and Northern Kenya regions. Attacks have increased in frequency since the Kenyan military was first deployed to Somalia in support of the Somali government's counterinsurgency campaigns in October 2011. This tension, combined with the government's huge and growing counterterrorism budget, has significantly expanded the Kenyan government's communications surveillance powers. Its defense and intelligence budget has shot up. In 2017, 124 billion KSh (around 959 million GBP) was allocated to the Kenya Defence Forces (KDF) and the

3 The CCK was renamed the Communications Authority of Kenya (CA) in 2014.

4 "Four years on, the battle to build a cohesive nation continues", National Cohesion and Integration Commission, 2012, available at: https://www.cohesion.or.ke/index.php/media-centre/press-statements/117-four-years-on-the-battle-to-build-a-cohesive-nation-continues

5 "CCK issues new rules to curb hate speech in campaigns," The Nation, 24 October 2012, available at: http://www.nation.co.ke/news/politics/CCK-sets-new-rules-to-curb-hate-speech-in-campaigns/1064-1594004-8r0fmm/index.html

6 "Phone firms block 300,000 hate texts daily, says Ndemo," The Nation, 21 March 2013, available at: http://www.nation.co.ke/news/Phone-firms-block-300-000-hate-texts-daily-says-Ndemo-/1056-1726172-bysv8uz/index.html

National Intelligence Service (NIS),[7] Kenya's primary signals intelligence agency, up from 98 billion KSh in 2016.[8] The United States' counterterrorism assistance to Kenya roughly tripled from 38 million USD in 2014 to 100 million USD in 2015,[9] while the United Kingdom's operational and financial support remains significant.[10]

The Kenyan government's counterterrorism operations have been particularly brutal and disproportionate. Security services arrested at least 4,000 majority ethnic Somali Kenyans [11] in during Usalama Watch,[12] a police operation "to curb the rising spate of terrorist attacks in the country." Scores of Kenyan citizens – most of them male, many of them Muslim – have been killed or 'disappeared' at the hands of Kenya's police in what is being called an epidemic of extrajudicial killings.[13] Domestic and international human rights groups as well as the constitutionally-mandated Kenya National Commission on Human Rights [14] have highlighted the role of the Police General Services Unit (GSU) and the Anti-Terrorism Police Unit (ATPU), in particular.

Abuses in counterterrorism are occurring against a backdrop of widespread law enforcement corruption and impunity. One in three Kenyans has been subject to ill treatment at the hands of the police, according to a 2016 study by the Kenyan Independent Medico-Legal Unit.[15] The Nation newspaper found that police officers killed 122 persons in the first eight months of 2016.[16] The government is also increasingly scrutinizing civil society groups as part of its counterterrorism

7 "Key highlights of the KSh2.3 trillion 2016/2017 Budget", The National Treasury, Government of Kenya, 8 June 2016, available at: http://www.mygov.go.ke/?p=10315

8 "National security budget shoots up as war on terror intensifies," The Nation, 16 October 2016, https://www.standardmedia.co.ke/article/2000219847/national-security-budget-shoots-up-as-war-on-terror-intensifies

9 "U.S. Counterterrorism Aid to Kenya," Security Assistance Monitor, 21 July 2015, available at: http://securityassistance.org/fact_sheet/us-counterterrorism-aid-kenya

10 "Inside Kenya's Death Squads", Al Jazeera Investigates, December 2014, available at: http://interactive.aljazeera.com/aje/KenyaDeathSquads/

11 "Somalis are scapegoats in Kenya's counter-terror crackdown", Amnesty International, 2014, available at: https://www.amnesty.org/download/Documents/4000/afr520032014en.pdf

12 "Revised Police Reforms Program Document 2015-2018," Ministry of the Interior and Coordination of National Government, August 2015, available at: http://www.npsc.go.ke/index.php/2014-03-25-12-08-21/downloads

13 See for example: "Extrajudicial killings an epidemic, Haki Africa says, details 81 cases," The Star, 7 December 2016, available at: http://www.the-star.co.ke/news/2016/12/07/extrajudicial-killings-an-epidemic-haki-africa-says-details-81-cases_c1469715 and "Kenya's Vicious War Against Its Youth," Foreign Policy, 14 March 2016, available at: http://foreignpolicy.com/2016/03/14/kenyas-vicious-war-against-its-youth/

14 Kenya National Commission on Human Rights, http://www.knchr.org

15 "Summary of the National Prevalence Torture Survey 2016," Independent Medico-Legal Unit, 2016, available at: http://www.imlu.org/2011-06-30-23-44-4/2015-08-28-09-08-23/reports.html

16 "Police kill 122 in 8 months, Nation Newsplex database shows," Daily Nation, 1 October 2016, available at: http://www.nation.co.ke/newsplex/police-killings-kenya/2718262-3401800-wrmh5az/. The regular and Administration Police (AP) were the most frequently implicated in these abuses, and most cases had no clear links to terrorism investigations.

campaign. In late 2014, it deregistered 500 civil society groups [17] for alleged registration irregularities and suspected fraud. Prominently critical Muslim human rights groups were deregistered and had their bank accounts frozen in April 2015;[18] the government claimed that they were linked to jihadist group Al-Shabaab.[19] Several lawyers and media professionals, too, have disappeared under suspicious circumstances.[20] The police has overtly questioned whether its critics support "the Kenyan people or terrorist groups".[21]

17 "Kenya De-lists 500 NGOs in Crackdown," Voice of America, 16 December 2014, available at: http://www.voanews.com/a/kenya-de-lists-five-hundred-non-governmental-organizations-in-crackdown/2561217.html

18 "Situation Analysis of MUHURI and Haki Africa," National Coalition of Human Rights Defenders –Kenya, 17 November 2015, http://nchrdk.org/2015/11/situation-analysis-of-muhuri-and-haki-africa/

19 The Kenya Gazette, Vol. CXVII, No. 36. 7 April 2015, available at: http://webcache.googleusercontent.com/search?q=cache:P18pjju7aHwJ:www.nation.co.ke/blob/view/-/2679390/data/987688/-/vn59cw/-/TERROR-LIST.pdf+&cd=1&hl=en&ct=clnk&gl=uk&lr=lang_en%7Clang_th

20 See for example the cases of journalist Bogonko Bosire, who disappeared in September 2013, and State House lawyer Albert Muriuki, who disappeared in December 2013. Administration Police officers are currently standing trial for the June 2016 murders of lawyer Willy Kimani, his client Josphat Mwenda and their driver Joseph Muiruri.

21 "Press Statement," Office of the Inspector General, National Police Service, 8 December 2016, available at: http://www.mygov.go.ke/?cat=100

Expanded Powers, But Short on Detail

Intelligence-gathering powers in post-independence Kenya were concentrated around the presidency and the Special Branch. In 1998, the National Intelligence Service (NIS) was created to replace the Special Branch; it is now Kenya's primary signals intelligence agency.[22] The Kenyan government's communications surveillance capacities were vague and opaque. Kenyan media published only anecdotal reports of surveillance throughout the early 2000s.[23] Yet the Kenyan government's increasing attention to domestic terrorism in the early 2010s ushered in important developments.

CA

COMMUNICATIONS AUTHORITY KENYA

The Communications Authority of Kenya (CA) is Kenya's telecommunications industry regulator. It officially oversees the management of the national telecommunications infrastructure.[24] Formerly called the Communications Commission of Kenya (CCK), the CA awards operating licenses to providers and monitors their regulatory compliance. The CA is also an important player in the development of Kenya's emerging Cybersecurity Policy framework – it sits alongside the NIS, KDF and ICT Authority among others on the National Cybersecurity Steering Committee. The CA is responsible for inspecting equipment used on telecommunications infrastructure.

22 "The Origins of the Intelligence System of Kenya", Brigadier (rtd) Wilson Boinett. In: Changing Intelligence Dynamics in Africa. Eds. Sandy Africa and Johnny Kwadjo. 2009. Available at: http://africansecuritynetwork.org/assn/download/publication/Changing%20Intelligence%20Dynamics%20in%20Africa.pdf?lbisphpreq=1

23 See for example: "Bugged - Police Can Now Listen to Your Phone Talks", The Standard, 9 September 2007, available at: http://allafrica.com/stories/200709100352.html

24 The Kenya Information and Communications Act (2011) sets out the then-Communication Commission of Kenya's authority. Available at: http://www.ca.go.ke/images/downloads/sector_legislation/Kenya%20Information%20Communications%20Act.pdf

"The war on terror has compelled the world to intrude into personal privacy," stated Michael Katundu, acting director of the then-Communications Commission of Kenya (CCK) in early 2012.[25] That year, news had leaked to the press that the CCK was engaged in building a system to monitor outgoing and incoming internet traffic with the support of the International Telecommunications Union (ITU). The press and legal profession were quick to note that the Network Early Warning System (NEWS) risked violating Kenyans' constitutional right to privacy (Article 31).[26] Kenya's operators, too, questioned their ability to protect their customers' privacy. But this project went ahead without substantive challenge or public debate about the program's actual capacities.

The National Intelligence Service Act and the Prevention of Terrorism Act

Two important acts in 2012 codified the government's interception capacities.[27] The National Intelligence Service Act (2012)[28] grants the Director General of the NIS the ability to intercept an individual's communications when he or she has 'reasonable grounds to believe' such information is required for an investigation subject to a prior application to the High Court for an interception warrant.[29] On the law enforcement side, the Prevention of Terrorism Act (2012)[30] granted police officers above the rank of a Chief Inspector the power to request an interception of communications order from the High Court. Worrying, however, was the power granted to the police to enter telecommunications operators' premises to install monitoring devices (art. 36). Left undefined, these devices could potentially capture far more than needed to track an individual or even a group of individuals.

25 "CCK Defends Plan to Monitor Private Emails," The Star, 17 May 2012, available at: http://allafrica.com/stories/201205181170.html

26 "CCK sparks row with fresh bid to spy on Internet users," Business Daily Africa, 20 March 2012, http://www.businessdailyafrica.com/Corporate-News/CCK-sparks-row-with-fresh-bid-to-spy-on-Internet-users-/-/539550/1370218/-/item/2/-/edcfmqz/-/index.html. Kenya's Constitution supersedes all domestic legislation, including the Kenya Information and Communications Act, which provided the legal basis for the system. The NEWS initiative was conceived as an initiative of the Global Response Centre of the ITU and was to be deployed in a number of countries worldwide. For more information about NEWS, see: https://webcache.googleusercontent.com/search?q=cache:2m1VWtARTd0J:https://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf+&cd=1&hl=en&ct=clnk&gl=uk&lr=lang_en%7Clang_th&client=safari

27 A full examination of Kenya's legal regime governing the interception of communications is beyond the scope of this investigation.

28 National Intelligence Service Act (2012), available at: http://kenyalaw.org/lex/rest//db/kenyalex/Kenya/Legislation/English/Acts%20and%20Regulations/N/National%20Intelligence%20Service%20Act%20No.%2028%20of%202012/docs/NationalIntelligenceServiceAct28of2012.pdf

29 Articles 36 and 42.

30 Article 36. Prevention of Terrorism Act (2012), available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/PreventionofTerrorism_No30of2012_.doc

The Westgate Mall terrorist attack provided a watershed moment for the expansion of the Kenyan government's surveillance powers. On 21 September 2013, gunmen stormed an upscale mall in Nairobi, killing over 60 and wounding over 170 in an attack later claimed by al-Shabaab. The Kenyan government soon embarked on an overhaul of its surveillance regime as part of a reexamination of the country's security policies.[31] The Kenyan government was set to gain its most significant powers to date.

The Security Laws (Amendment) Act 2014

In December 2014, the Kenyan Parliament passed a hastily-debated omnibus security bill, the Security Laws (Amendment) Act. The Act casts some doubt on what was previously a clear requirement for all agencies authorized to intercept communications to obtain prior judicial warrants.[32]

The Security Laws (Amendment) Act introduced a new amendment to the Prevention of Terrorism Act: a Cabinet Secretary was tasked with making new regulations to govern communications interception by the "national security organs" when related to terrorism investigations.[33] The "national security organs" are defined widely in Article 239 of the Constitution as the Kenya Defence Forces, NIS and the Kenya Police Service. It is unclear if these rules, which have yet to be articulated, would still require the National Security Organs to obtain warrants to intercept communications, as set out in previous laws.

31 See also: "Beyond Westgate: Security and Accountability in Kenya", Dr. Awino Okech, African Security Sector Network, 12 March 2014, available at: http://africansecuritynetwork.org/assn/beyond-westgate-security-and-accountability-in-kenya/ and "Deputy President William Ruto on Media Law", Office of the Deputy President, 3 November 2013, available at: http://www.deputypresident.go.ke/index.php/press-briefings/deputy-president-william-ruto-on-media-law

32 See also analysis by FIDH. "Kenya: The Security Laws (Amendment) Act must be repealed", FIDH, 19 December 2014, https://www.fidh.org/en/region/Africa/kenya/16696-kenya-the-security-laws-amendment-act-must-be-repealed

33 Article 69, Security Laws (Amendment) Act (2014), reads: "The Prevention of Terrorism Act is amended by inserting the following new section immediately after section 36- 36A. (1) The National Security Organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary. (2) The Cabinet Secretary shall make regulations to give effect to subsection (1), and such regulations shall only take effect upon approval by the National Assembly. (3) 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." Available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2014/SecurityLaws_Amendment_Act_2014.pdf

The Security Laws (Amendment) Act also expanded the intelligence services' powers by introducing a specific section on "Special Operations"[34] related to national security. Covert operations can be initiated by the Director General of the NIS. Under his orders, any member of the intelligence service of any rank could monitor communications as well as seize essentially any material from private property. Again, communications interceptions would be carried out with written authorizations issued per "guidelines approved by the [National Security] Council", which are still unclear. Officially, and confusingly, given the article 69 amendment discussed above, authorization for covert operations including to 'monitor communication' would still require a High Court warrant.

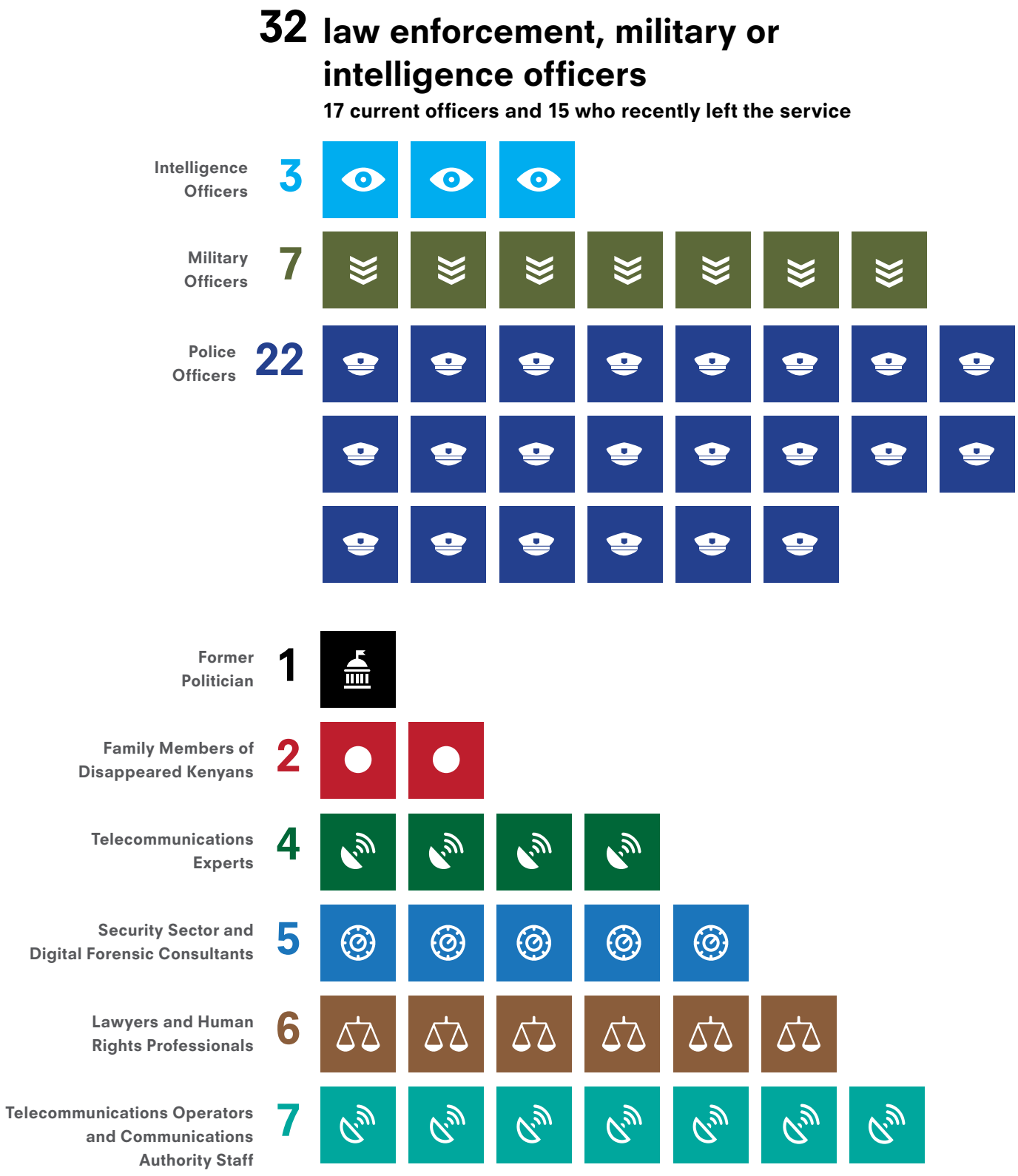
The government slipped the omnibus bill through at the Christmas season with very limited public consultation, prompting opposition-led protests at the national assembly.[35] The bill passed. Despite a successful constitutional challenge to certain provisions in the law,[36] the new communication interception powers emerged untouched.

34 Article 56.

35 "CORD and Jubilee clash over security bill", The Standard, 17 December 2014, available at: http://www.standardmedia.co.ke/article/2000145035/raila-odinga-takes-on-uhuru-kenyatta-over-security-bill?articleID=2000145035&story_title=cord-and-jubilee-clash-over-security-bill&pageNo=3

36 "Security laws illegal, declares High Court," The Daily Nation, 23 February 2015, http://www.nation.co.ke/news/politics/Security-laws-illegal-declares-High-Court/1064-2633342-jw2qp1/index.html

Privacy International interviewed or reviewed firsthand testimony from 57 individuals. This report is the first of three PI investigations in Kenya.



Spying First, Then 'Making it Proper'

In practice, if not in law, Kenya's surveillance regime appears bifurcated. The NIS intercepts both communication content and acquires call data records without warrants to gather intelligence and prevent crime, and police agencies acquire communications data with warrants to prepare criminal cases.[37] If it's 'just' for intelligence, explained one police ATPU investigator, then warrants are not sought: "For the sake of investigations, the DCI [Directorate of Criminal Investigations officer] attached to Safaricom will just give [it to] you… When you take someone to court, you have to make it proper now." Safaricom stated to PI that they "only provide information as required by courts...and upon receipt of relevant court orders." Safaricom's full response is included as an annex.

Intercept (s36)

A 2015 ATPU investigation manual seen by Privacy International demonstrates the official distinction between how the police and the intelligence service can intercept communication

The manual authorizes police ATPU officers to use intercept powers of section 36 of the Prevention of Terrorism Act (2012) to investigate 30 different terrorism-related offences. ATPU officers have been credibly accused of human rights abuses including torture.[38] The manual also notes that while the ATPU can intercept communications only with written consent of the Inspector General of Police, and an ex parte application to a Chief Magistrate of the High Court, it states that the NIS "can also intercept…but regulations still need to be issued by the CS [Cabinet Secretary] for this to take effect." No such regulations have yet been issued.

Credit: Seen by Privacy International. November 2016.

If only the distinction between intelligence gathering and trial preparation were so clear. In reality, the NIS often tips off the police based on information gleaned from its own communications monitoring, the police then obtain the necessary clearance to re-surveil the same target to produce evidence admissible in court, according to prosecution and defense attorneys and police investigators. That is, if a suspect ever gets to court.

37 The police also do have a limited capacity to intercept communications content, which is discussed in the section "Closing in."

38 "Deaths and Disappearances: Abuses in Counterterrorism Operations in Nairobi and in Northeastern Kenya", Human Rights Watch, 19 July 2016, available at: https://www.hrw.org/report/2016/07/19/deaths-and-disappearances/abuses-counterterrorism-operations-nairobi-and

Telecommunications operators end up handing over their cusomers' data because they largely feel that they cannot decline agencies' requests, in part due to the vagueness in the law and accompanying telecommunication industry regulations. Several telecommunications operators spoke of the threat, either direct or implicit, that their licenses[39] would be revoked if they failed to comply.

The Registration of Subscribers of Telecommunications Services Regulations (2014) of the Kenya Information and Communications Act (KICA, 1998) impose data disclosure requirements on operators. An operator is required to provide the CA "access to its systems, premises, facilities, files, records and other data to enable the Commission inspect" them.[40] It is unclear what, if any, limitations there might be as to the 'data' the operator is compelled to provide. The KICA (1998) prevents operators from disclosing individuals' or businesses' private information without their consent – except in connection to criminal investigations or proceedings, among other situations (section 93).[41] But does this obligation to not disclose private client data extend to requests by the NIS, which does not gather intelligence for criminal investigations, as the police does?

One internet service provider recalled the difference between his experiences with the police and with the NIS: "A [police] agency comes to me, and they give me the Occurrence Book (OB) number of the case they are investigating…. The NIS has unfettered access to data." The NIS simply contacted this operator for the data it required. "They will say 'give us [data for] whenever X calls Y over this time period', for example…In instances involving terrorism, no warrants are produced. We have to comply or there is the threat that our licenses [will] be revoked." A Communications Authority of Kenya (CA) officer confirmed his account: "they'll get their license revoked [if they do not comply]... If I were them, I'd comply too".

39 Condition 16 of the Application Service Provider License states that the CCK's licensees "are prohibited from recording, silently monitoring or intruding into its Subscriber's communications traffic…" (16.3). Yet section 16.4 adds a blanket exception to the rule: "Except for the purposes of law enforcement," the Licensee is required to let parties know if their traffic is to be recorded, monitored or intruded into. Section 13.2 adds an even more wide-ranging exception in case of national security emergencies: "In case the emergency or crisis is related to aspects of national security, the Licensee shall coordinate with the competent entity indicated by the Commission and provide necessary services…" The then-CCK cited this 'national security' exception in letters seen by Privacy International asking providers to comply in installing the NEWS traffic monitoring system. The NEWS project was no small infrastructural feat – the relative permanence of both it and the 'emergency' powers that the CCK claimed underpin it, betrays how the government conceives the state of emergency to be similarly permanent.

40 Section 13, the Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations 2014

41 Section 31 of KICA (1998) also prohibits licensed telecommunication operators from intercepting messages sent through licensed telecommunication systems.

Telecommunications operators often perceive that they have a duty to preserve national security. "No one's going to say no," says a senior source at one of Kenya's mobile operators. "And think about it. If one of the guys who attacked Westgate was using the [mobile operator's] money SIM card, who am I to say no?... I'll give it up very clearly… If the NIS just shows up at 2 o'clock on a Tuesday afternoon, we're investigating, and we need all this, for all these numbers, that I know nothing about? What the hell am I supposed to do?"

On Your Marks: Infiltrating Telecommunications Networks

Direct access

The police services and NIS can access Kenyans' communications data formally, with the consent and cooperation of telecommunications operators. But the NIS also has direct access to Kenya's telecommunications networks, which allows for the interception of both communications data and content.[42] Direct access[43] describes situations where state agencies have a direct connection to telecommunications networks which allows them to obtain digital communications content and data (mobile and/or internet), without prior notice or judicial authorisation and without the

Direct Access

In most countries, telecommunication service providers are legally required to put in place the technical means for individual communications to be intercepted for investigation purposes. Service providers often need to purchase and install (or allow to be installed) on their networks mediating devices that are compliant with one or more international interception standards. In 2015, the European Court of Human Rights issued a judgement warning that direct access systems are prone to abuse. It stated in the case of Roman Zakharov v. Russia that "a system… which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorization to the communications service provider or to anyone else, is particularly prone to abuse."[44]

42 The Vodafone group stated that it had not received any Kenyan agency or authority demands for lawful interception assistance. Vodafone is the majority owner of Safaricom, Kenya's most popular mobile service provider. Given that it is widely acknowledged, including by law enforcement, that communications and communications data can be intercepted (though this report is the first to closely examine how), Vodafone's admission if correct would strongly suggest that Kenyan authorities have some form of direct access to Safaricom's network. See: "Law Enforcement Disclosure report" in Sustainability Report 2013/4, Vodafone Group Plc, 2014, pp.74. available at: https://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf

43 "Submission to the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Study on Telecommunications and Internet Access Sector," Privacy International, 30 November 2016, available at: https://www.privacyinternational.org/node/1003

44 European Court of Human Rights, Roman Zakharov v. Russia judgement (4 December 2015) para 270. http://hudoc.echr.coe.int eng#{%22fulltext%22:[%22zakharov%22],%22documentcollectionid2%22:[%22GRA NDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-159324%22]}

involvement of the telecommunications provider or internet service provider that owns or runs the network. Direct access poses both legal and technical challenges. Direct access has a defined link to arbitrary and abusive practices that impact freedom of expression and privacy.

Access at The Telecommunications Providers

In Kenya, law enforcement agents are physically present within telecommunications operators' facilities, formally, with providers' knowledge. NIS agents are also informally present in the telecommunication operators' facilities, apparently undercover, according to current and former Safaricom, CA, and NIS staff interviewed by Privacy International.

The major telecommunications providers have at least one law enforcement liaison, a police officer of the Directorate of Criminal Investigations (CID) on secondment. This analysis focuses on Safaricom, by far Kenya's most popular mobile service provider with over 60% of the market share. At Safaricom, around ten CID officers sit on one floor of the Safaricom central bloc. They provide information to all police branches.

Safaricom also has civilian investigators who sit within the Ethics and Compliance Department[45] of Safaricom. These investigators' primary responsibilities are to follow up fraud and misuse allegations on behalf of Safaricom, and to assist their law enforcement colleagues in cases in which criminal action may have occurred. Through an interface, Safaricom officers can query a database that collects information from Safaricom's call data records, SIM registration, mobile money, and subscriber registration databases. Law enforcement liaison officers are separately able to input requests into a query queue; the interface will render data according to the priority/time it was submitted, according to police investigators and Safaricom staff. Standard call data records list the phone numbers of the initiating and receiving devices, the location of the base transceiver station (BTS), the type of communication (whether call or SMS), and the duration of the call. Safaricom stated to PI that "only authorised Safaricom staff have access to systems and tools that can access confidential customer information and this access is controlled and monitored."

Officially, law enforcement requests for data to Safaricom require a letter of justification, written by an investigating officer, signed by his or her superior, and provided in hard copy or emailed to the Safaricom law enforcement liaison, according to current and former police investigators. The reason does not, however, have to be detailed – often a statement of the category of crime under investigation will suffice.

45 More information about the Ethics and Compliance Department is contained in Safaricom's 2015 Sustainability Report, available at: https://www.safaricom.co.ke/sustainabilityreport_2015/public/uploads/Governance,%20risk%20&%20regulation.pdf

But agents routinely circumvent protocol in urgent cases. In these cases, information is immediately rendered. One ATPU officer explained, "[i]f it's national security, whatever, we will breach protocol. … if it's urgent, you just make a call. 'Talk to my boss'…So my boss talks to the charge of security there, and we are given the data, the contact immediately….in a matter of minutes." Safaricom deny this claim. Live tracking of an individual mobile phone's location can also be performed within Safaricom by using BTS data – this often allows operational teams to hone in on an area and deploy mobile interception devices to further pinpoint a target's location. "We normally don't do this ourselves," explained a police officer. "We have IT experts there. Mostly civilians from Safaricom. They are really, really trained." Safaricom deny this claim.

The reported presence of NIS officers undercover in Safaricom and possibly other telecommunication network operators presents serious concerns as to whether any civilian authority or mechanism would be able to effectively oversee the process of communications interception. "The way we know they are here is that they'll be present, seconded from somewhere else, but then suddenly they'll disappear," explained one CA employee. "And then you hear your colleagues saying 'didn't you know, that guy was NIS?' They keep very much to themselves. You'll even find your boss some time suspecting you of being NIS." According to sources, by building rapport with civilian officers, NIS are able to informally access communications data. "Of course [the NIS officer in Safaricom] will liaise with the Safaricom engineer... Once there is information that he needs, or that our office needs, he gets in, he talks to the engineer, he is given access," explained a current NIS officer." Because in Safaricom, every time you log into the database to check for a certain number, you have to put your code there. … It depends on the rapport he has with the engineers…. They trust him."[46]

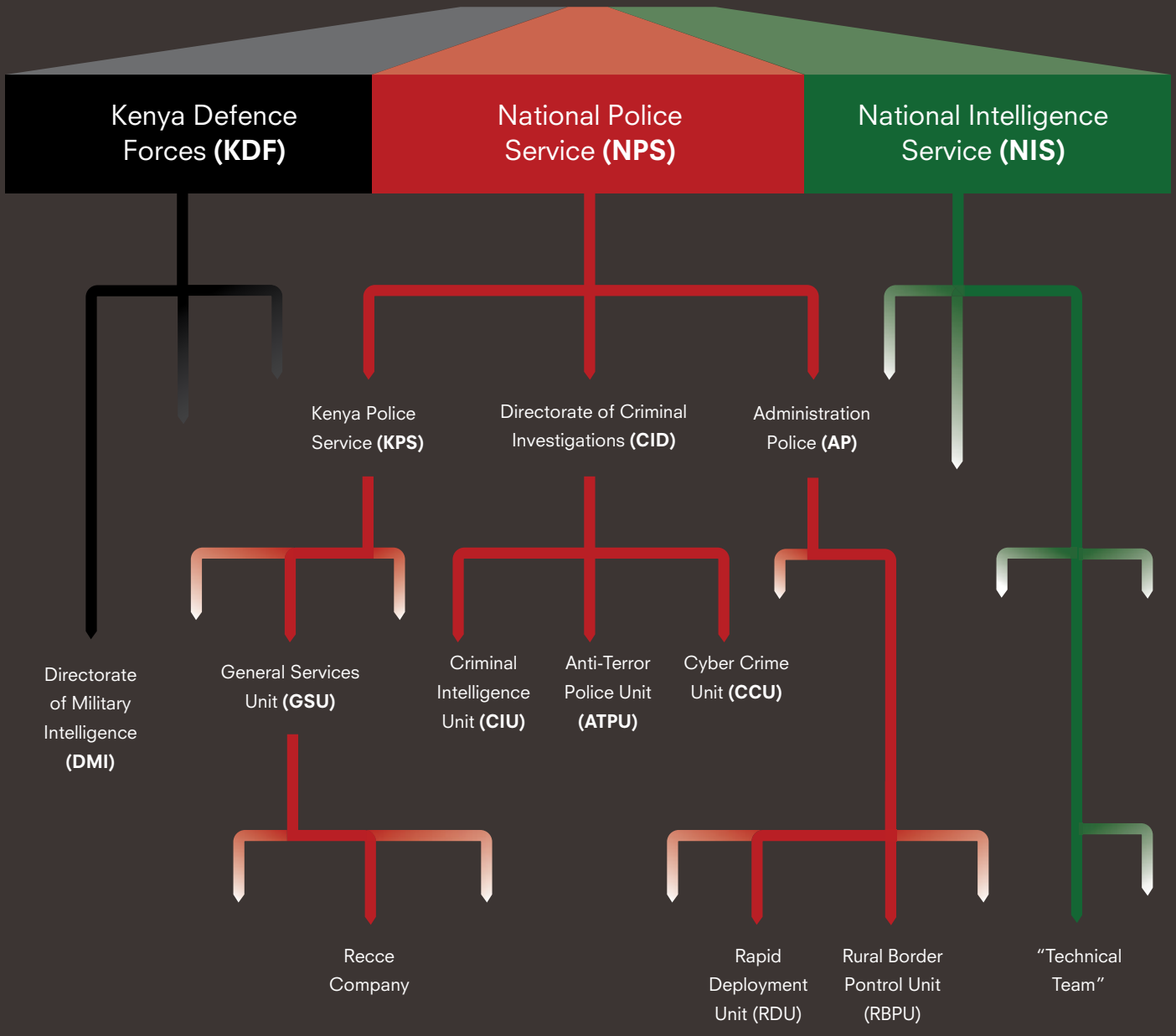
Responding to Privacy International, Safaricom CEO Bob Collymore stated that Safaricom "ha[s] no relationship with NIS as relates to communication surveillance in Kenya; and we do not have any officers or other representatives of the NIS who are employed, formally or informally, at Safaricom," Safaricom's full response is included as an annex.

46 Another former NIS employee confirmed that NIS agents were placed in telecommunications network operators. Two telecommunications providers also described informal NIS requests for information, which they granted. One described it as: "I believe in building relationships, right?... I try and get you to the point of understanding what I can and cannot do according to what I understand is supposed to happen. It really depends on how they [NIS] come in. ...There are some who are very aggressive."

Flagging Targets

The NIS is also passively connected to Kenya's telecommunications backbone. NIS agents analyse and listen to live calls at NIS offices both regionally and in Nairobi, as described by two NIS sources and confirmed by a CA officer. Sources described how NIS-owned BTSes directly access Kenya's telecommunications backbone. Sources confirmed their presence in operationally important areas, such as Mandera on the border with Somalia and Mombasa, on Kenya's coast. Mobile phone numbers of interest will be 'flagged' such that they notify the NIS system when they are engaged in a call. "Once we get a red light on this particular person," stated one NIS agent, "we try checking the contents of his conversation. If it's trash we just discard it. If it's something of interest, we make a move and follow it up." This enables agents to selectively listen in to and record conversations, described two NIS officers. Analysis centres in Nairobi include one office in the Westlands neighborhood, proximate to Safaricom, as well as at the NIS headquarters off Thika road. Targets are reportedly unaware of the operation, according to several former NIS officers. The Office of the President and an NIS representative did not respond to Privacy International's requests for comment.

National Security Council



These agencies across the military, law enforcement and intelligence services are engaged in either conducting communications surveillance, or using information gained from communications surveillance in operations. This diagram does not contain all relevant units; it focuses on those highlighted in the report.

Source: Kenya government websites, PI sources. 2017.

Getting Ready: Sharing Intel and Preparing Ops

The Kenyan government coordinates its counterterrorism efforts through various mechanisms. One is the Joint Operations Centre in Jogoo House, the National Police headquarters.[47] The inter-agency centre functions as a triage platform for pieces of operational intelligence, including information derived from communications surveillance.

The NIS, the primary agency responsible for performing communications surveillance in Kenya, and the agency with the most sophisticated means to do so, feeds information to other agencies which is directly used in counterterrorism actions.

"[NIS] come with information, but they don't tell us how they got the information...", explains an ATPU officer. "They tell us content, [like] 'around 7, there are people who will come there pretending to be guests at the hotel, we suspect they are terrorists.'" Often this information suggests it was gained through communications surveillance – it contains phone numbers or detailed statements individuals' communication patterns. Despite the crucial role of NIS in providing operational intelligence to law enforcement units, agents working for other branches largely report that they are not aware of exactly what the NIS do and they gather their information. "NIS? …In all the years I have worked, I have even interacted with them, I really don't know their capabilities…" recalls a forensics expert familiar with the police. "Once that open guy transfers services to the other agencies, he then zips up."

Communications surveillance powers are concentrated around the agency – NIS – that is subject to the least oversight. The NIS is subject to a parliamentary oversight through "the relevant committee," presumably the Intelligence and Security Committee.[48] The NIS Act (2012) also established an Intelligence Service Complaints Board, comprising a high court judge, a nominee of the Kenya National Commission on Human Rights, an advocate, a retired intelligence officer, and a senior public servant.[49] But

47 The Joint Operations Centre is not the same as the Command, Control and Communication (IC3) centre, which is housed on a different floor at Jogoo House. The IC3 centre is a police coordination initiative that features a critical incident management system, emergency call centre, dispatching centre, and data centre, where data from a network of CCTV cameras deployed nationwide is collected and analysed. See: "Director Command, Control and Communication (IC3) Centre", National Police Service, 2017, available at: http://www.nationalpolice.go.ke/2015-09-22-11-51-11/director-command-control-and-communication-ic3-centre.html

48 s. 65, National Intelligence Service Act (2012).

49 s. 66-67 National Intelligence Service Act (2012).

apart from receiving and investigating complaints, the Board is limited to making recommendations to the President or Cabinet Secretary. Very little information is publicly available about the Board and its investigations, if it has engaged in any.

In practice, the NIS is an agency that is almost entirely opaque even to the senior agents of other security organs with whom the NIS is mandated to work. These security organs are, to a large degree, dependent on the NIS to carry out communications surveillance. This effectively renders meaningless whatever legal requirements or operating procedures that do exist that would require an agent to obtain an interception warrant, or follow another accountability process.

Kenya's communications surveillance capacities do not yet appear to have reached the scale of massive, automated collection and storage of call content and data. The government's relatively targeted approach to surveilling individuals is no less concerning, however. The NIS share information liberally with police units engaged in grave human rights abuses. Information obtained through communications surveillance is central to the identification, pursuit, and 'neutralisation', or killing, of suspects – a process in which Kenyan citizens' fundamental human rights are seriously abused, as the next section will show.

Closing In: Surveillance In Kill Or Capture Operations

This section explores the use of surveillance technologies and intercepted communications in the cycle of tracking, arresting, killing, and investigating terrorism suspects.[50] Terrorism suspects are frequently arrested, subjected to torture, deprived of counsel, and killed. In some operations, a dedicated paramilitary police squad of GSU Recce Company and the ATPU carry out targeted operations whose aim, according to officers, is to kill suspected terrorists.[51] As described to Privacy International, these operations are in part facilitated by location data derived from mobile phone signals, as well as information derived from call data and call content analysis. This information is largely provided by the NIS, which conducts communications surveillance, as described above.

Units of the NIS, Directorate of Military Intelligence (DMI) and CID all have (or had) mobile devices used to track targets, collect communications data and listen into live communications for operational purposes.[52]

Field Tracking

The NIS currently have devices that allow an agent of the small NIS technical unit to geolocate a target through his/her mobile phone. The system appears to consist of a handheld device, roughly the size of a large mobile phone that communicates through an interface operated by analysts at NIS' headquarters off Thika road, according to one NIS officer and an expert. This NIS interface is linked to a database which contains live BTS location data, and call data records. One NIS officer described how this system functions "by satellite" to give an approximate location for a mobile device, which then allows agents to move closer to the target to perform more targeted surveillance.

> "[The handheld device] is synchronized to the machine in the office… the phone, it's synchronized to the machine… You will be able to get the [target's] number, who [he is] communicating with. Where [his] location is. It is able to receive all the communications. It is able even to get to know what stuff you are communicating with somebody else."
>
> **NIS Officer**

50 The focus of this report is on Kenyan actors. Privacy International also documented significant evidence of UK and US support to and direct involvement in counterterrorism operations, including communications surveillance activities. However, we are abstaining from publishing on this issue until further verifying and elaborating on the facts at hand.

51 "Inside Kenya's Death Squads", Al Jazeera Investigates, December 2014, available at: http:// interactive.aljazeera.com/aje/KenyaDeathSquads/

52 There are also reports that the Kenya Anticorruption Commission (KACC) had also acquired similar devices. "Bugged - Police Can Now Listen to Your Phone Talks," The Standard, 9 September 2007, available at: http://allafrica.com/stories/200709100352.html

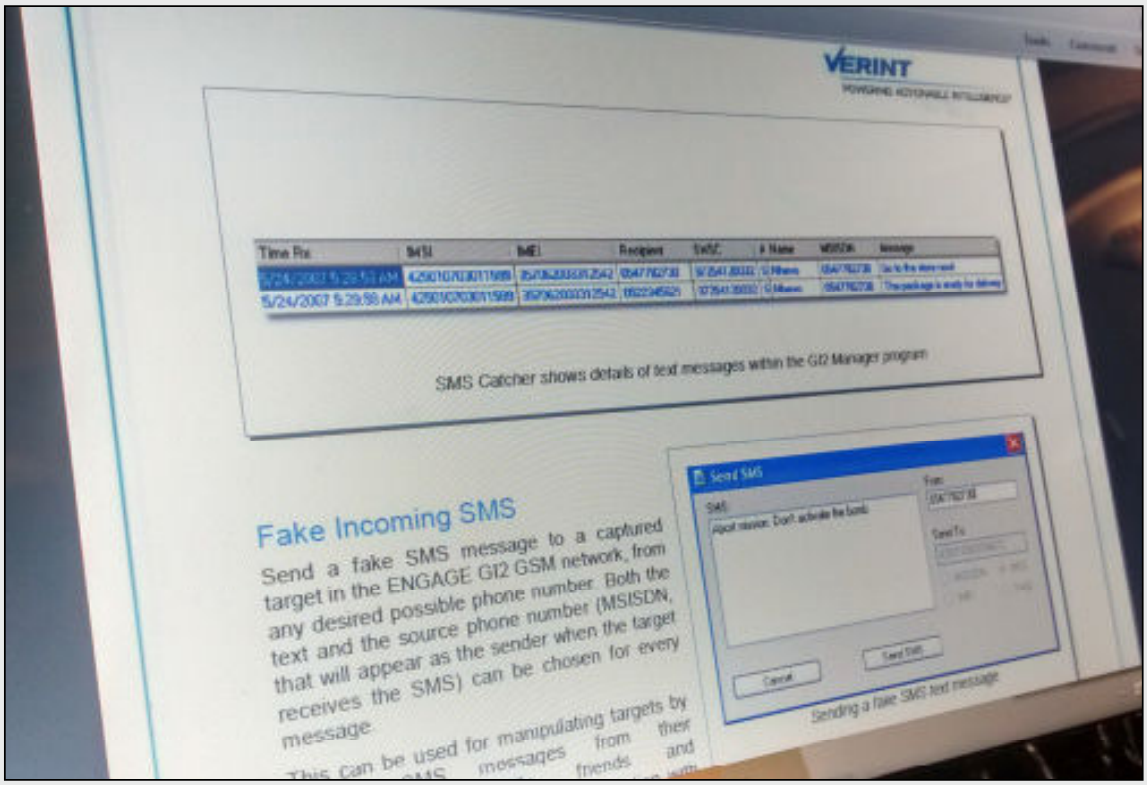
Several sources also described that the NIS have a device contained in a vehicle which appears to function like an IMSI catcher.[53] An IMSI catcher is phone monitoring equipment that is able to actively intercept communications "off-the-air" of surrounding devices. An IMSI Catcher performs interception by presenting itself as a base station amongst the mobile network: the station that your phone connects to when it wants to place a call or send a message. The IMSI Catcher mimics a base station by entering the network as the most powerful base station available, meaning that all mobile phones operating within the same area connect to the IMSI Catcher's base station. Once connected to the IMSI Catcher's base station, the Catcher has the mobile phone provide its IMSI and IMEI data. Once these details have been gathered it becomes possible to monitor the operation of the phone: the voice calls taking place, the messages being sent and the location of the phone.

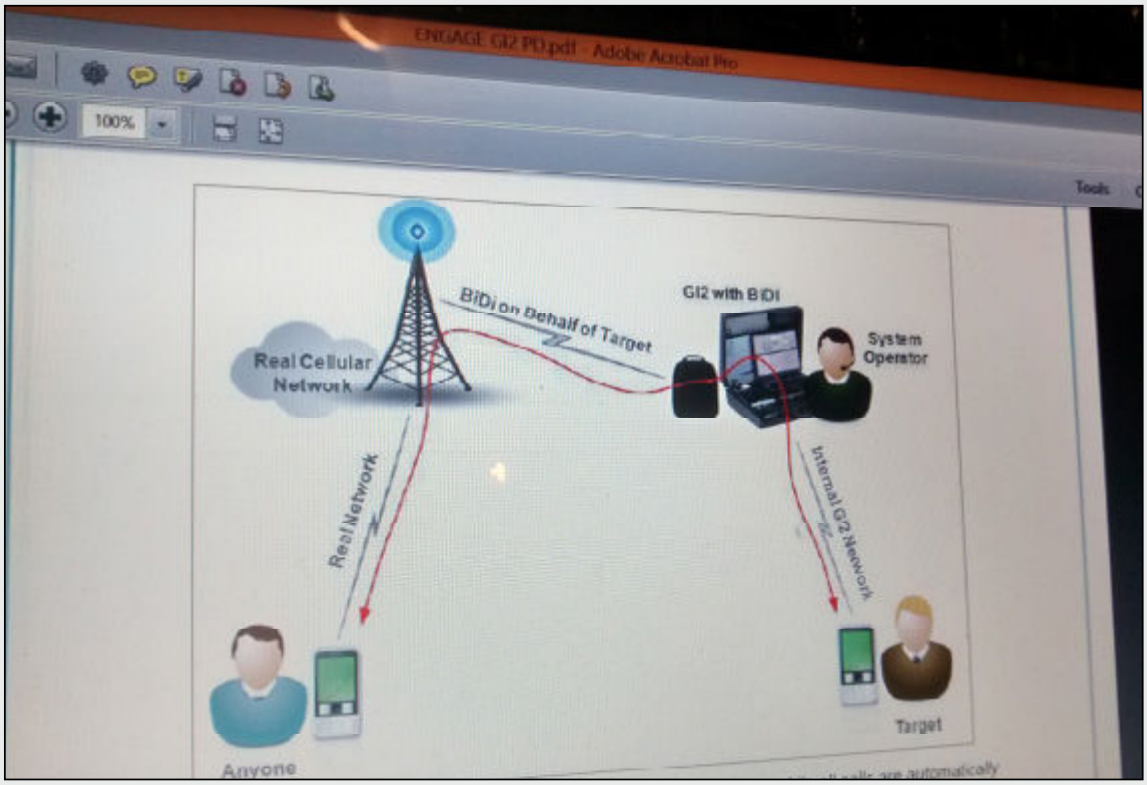
Military Intelligence (DMI), too, has a device that functions essentially like an IMSI catcher. It can intercept live phone calls provided the agent is within the range of the BTS with which an individual target's device is communicating. The DMI also monitors radio frequencies as it primarily focuses on gathering operational intelligence in rural areas near the Somali border areas of northeast Kenya. For this it uses the 'Blackbird' product, a "Signal Search, Collection, Geolocation and Analysis System" of American spectrum monitoring company SPX. SPX did not respond to Privacy International's request for comment.

The CID also had mobile off-the-air interception devices, at least in the period 2010-2011, provided by Israeli tech company Verint. "They don't need to get your device. All they need to do is get your number, they have a connection with the service provider, and they are able to get the cell location," explained one former officer, describing the Engage line of products.[54]

53 Recalls one former NIS agent: "It was Mercedes Benz, it was fitted with the equipment, it was able to tap those calls…We had the engineers inside the vehicle. They communicate with the engineers at the base." Another expert described two similar mobile devices contained in cars. One is an IMSI catcher under NIS control, which when not in operation is kept at the NIS HQ off of Thika road, in east Nairobi. The second is an IMSI catcher which also functions as a signal jammer. This device is under the control of the Presidential Escort Unit, and will accompany the Presidential convoy. PI was unable to confirm the number and make of IMSI catchers in Kenya. In 2007 it was reported that the NIS was the first agency in Kenya to have acquired mobile interception technology. See: "Bugged - Police Can Now Listen to Your Phone Talks," The Standard, 9 September 2007, available at: http://allafrica.com/stories/200709100352.html

54 A 2013 Verint brochure describes some of Engage GI2's capabilities: "Listen to, read, edit, and reroute incoming and outgoing calls and text messages (A5/1 and A5/3 encryption; Remotely activate a mobile phone's microphone; Identify the presence of target mobile phones". See: "Tactical Off-Air Intelligence Solutions," Verint, 2013, available at: https://www.documentcloud.org/documents/885760-1278-verint-product-list-engage-gi2-engage-pi2.html





Promotional material from Verint provided to the Kenyan police demonstrates the surveillance capacities of its Engage Gi2 product. Engage Gi2 devices were reportedly provided to the Kenyan CID and it is unclear if the devices are still in use.

Credit: January 2017. Obtained by Privacy International.

Kenyan officers tasked with procurement travelled abroad as guests of Verint's Israel office and to trade fairs, according to documents seen by Privacy International. Verint did not respond to Privacy International's request for comment.

The CID does, however, have global positioning radio system devices that can determine the precise location of a cell phone based on a triangulation between base stations, according to three different sources. It is unclear if the devices are also used to intercept phone calls, though their use must signed off by a senior official, with two CID sources indicating that this must be the head of the CID's Criminal Intelligence Unit, Abubakar Maalim. These are used primarily for high-value offenses such as kidnappings.

Intelligence gained by intercepting phone communications, primarily by the NIS, is provided regularly to units of the police to carry out counterterrorism operations, particularly the GSU-Recce company and Anti-Terrorism Police Unit (ATPU). These police units have significant and well-documented records of grave human rights abuses.

Kill or capture

Officers of the Recce Company[55] have admitted to carrying out extrajudicial killings as a matter of policy. ATPU[56] officers have also been linked to extrajudicial disappearances. The ATPU routinely engages in physical and psychological torture of its detainees, many of whom have disappeared.[57]

The Kenyan government relies on the paramilitary GSU-Recce Company in sensitive cases. The unit was created as a paramilitary force to protect Kenya's first president, Jomo Kenyatta, with support from the British SAS.[58] The NIS will direct them to where to "do their work", in part by tracing the target's location and intentions through their phones, and by leading pre-operation briefings. One former ATPU officer summarized the division of labor as "the people who identify targets are NIS. They take guys from Recce. They [Recce] do operations."

55 "Inside Kenya's Death Squads", Al Jazeera Investigates, December 2014, available at: http://interactive.aljazeera.com/aje/KenyaDeathSquads/

56 The Error of Fighting Terror with Terror", Kenya National Commission on Human Rights, September 2015, available at: http://www.knchr.org/Portals/0/CivilAndPoliticalReports/Final%20Disappearances%20report%20pdf.pdf

57 See various reports by the Kenya National Human Rights Commission, Human Rights Watch, and the Independent Medico-Legal Unit.

58 "How the Recce unit to protect Kenyatta was mooted and trained," The Nation. 11 December 2016, available at: http://www.nation.co.ke/news/How-the-Recce-unit-to-protect-Kenyatta-was-mooted/1056-3481946-9rv3rc/

A former Recce unit operative recalls that the hit squad would meet with ATPU and NIS officers before an operation. Another senior officer recalls: "The person who will be having the information is the person who has been doing the surveillance, who is NIS. So they will give the first briefing."

Beyond briefings, NIS agents are also actively involved in some operations. "While we are working, we move with the ATPU," explains one NIS officer. "We tell them 'ok fine. This is the info that we have.' …They [ATPU] can't get actually get to know, what are [the targets] discussing about, you know? Now, when it comes to the point of arrest, the ATPU will take over. …We [NIS] tell them 'the mark is here. He's dressed this way.' They just get him, pick him, no questions."

The Administration Police (AP),[59] too, rely heavily on NIS intelligence. "These guys are so important to us, eh? These guys from the National Intelligence Service," recalls one senior officer at the National Police Service. "They normally start with 'the intelligence reports we are receiving, blabla has been in contact with someone across the border.'" Several units of the AP, including the Rural Border Patrol Unit (RBPU) and Rapid Deployment Unit (RDU), are active in counterterrorism operations and have been accused of serious human rights violations, including abducting civilians.[60]

When it comes to operations, "they [the NIS] are the ones who give the intel most of the time," explains a former Recce officer. "They come, they mount the machine in the car and they move around…It will tell you location but not your exact location. Because it goes with what we call these Safaricom boosters [BTS]…As you approach there is what we call a sensor that [says] 'we are close,' depending on the signal, they can tell we are like 10 meters from the guy. So that is the time now the guys can disembark…and manually cordon the area."

NIS and ATPU investigators then will search the scene for evidence, including communications devices. The ATPU is responsible for taking custody of any captured suspect or person of interest.

The ATPU have been credibly accused of committing grave human rights abuses including torture. The ATPU carries out interrogations often, but not always, under

59 The AP is a paramilitary security unit. Despite its name, the AP falls outside the Kenya Police Service, and answers to the Ministry of Interior and Coordination of National Government, instead of the Police Inspector General. Its three main unites are responsible for emergency response, border patrol and security, and government building security.

60 "Deaths and Disappearances: Abuses in Counterterrorism Operations in Nairobi and in Northeastern Kenya", Human Rights Watch, 19 July 2016, available at: https://www.hrw.org/report/2016/07/19/deaths-and-disappearances/abuses-counterterrorism-operations-nairobi-and

NIS direction or with NIS agents present. Interviews are recorded. Phones are seized and examined. This often occurs without the presence of a lawyer. "The phone is taken to NSIS and they listen to the conversations and make a conclusion," recalled a former Recce officer. NIS are sometimes present during interrogations, particularly of high value detainees. "Why should you sit back and watch while you are the one who requires that [information]?" replied one former NIS officer.[61]

> "We just work under their shadow… we [ATPU] do what they [NIS] decide."
>
> **An ATPU officer**

Not many suspects make it to court. They often disappear.[62] Communications data, mostly intercepted by the NIS, is central to the whole counterterrorism cycle: identifying and tracking individuals, preparing and carrying out arrests and killings. It is unclear whether the interception of this information is subject to prior judicial approval, though several sources indicate that it is generally not.

A far better oversight regime is needed to minimize the Kenyan government's abuse of its communications surveillance powers, abuses which directly facilitate the commission of torture and extrajudicial killings – crimes under Kenyan law. The Office of the President, the National Police Service, and an NIS representative did not respond to Privacy International's requests for comment.

61 One ATPU officer described that NIS will independently detain individuals, during which time they are badly treated: "In the process of arresting, the NIS guys, before they hand a suspect to us, they try to get as much information as they can, that maybe they don't want us to get…They can even take them to a secluded areas, in the bush, they extract information, they do a lot of things, then they brought them [to us]…So in those kinds of rounds they make with the suspect, you never know what they do to them."

62 See for example: "KNCHR report: 25 killed, 81 missing in anti-terror operation", The Standard, 15 September 2015, available at: http://www.standardmedia.co.ke/article/2000176419/knchr-report-25-killed-81-missing-in-anti-terror-operation and "Kenya: Killings, Disappearances by Anti-Terror Police," Human Rights Watch, 18 August 2014, available at: https://www.hrw.org/news/2014/08/18/kenya-killings-disappearances-anti-terror-police

Elections and Accountability

New Security Measures

Kenyans will head to the polls in August to vote in Presidential elections. While the nation hopes for a smooth transition, many Kenyans fear a return to the sectarian violence of the 2007-2008 period, which saw over 1,000 Kenyans killed and 600,000 displaced.[63]

Kenya's Communications Authority has cited this risk to justify a 2 billion KSh (15.2 million GBP) investment in monitoring Kenyans' communications and communications devices.[64] The CA claimed in a January 2017 announcement that the three projects – one each to monitor radio frequencies, monitor social media platforms, and 'manage devices' – would prevent a repeat of the post-election violence of the 2007 election period. The telecommunications industry reacted strongly against the measures.[65] CA authorities rushed to assure that the projects would only be used to enforce regulatory compliance.[66]

Device Management System

In February 2017, details of the third project, a "device management system", were leaked to the press.[67] Telecommunications industry watchers alleged the system was

63 "Death Toll in Kenya Exceeds 1,000, but Talks Reach Crucial Phase," The New York Times, 6 February 2008, available at: http://www.nytimes.com/2008/02/06/world/africa/06kenya.html

64 "Kenya's communications authority to monitor private talk and texts during poll", The Standard, 13 January 2017, accessed on 13 January 2017 at: https://www.standardmedia.co.ke/article/2000229727/communications-authority-to-monitor-private-talk-and-texts-during-poll The link has since been removed from the Standard's site. It in the article, CA head Francis Wangusi is quoted as stating: "We have spent Sh1.1 billion on a spectrum monitoring system that will help us monitor unauthorised broadcasts coming from rural areas of the country…We have also spent around Sh600 million on a social media monitoring system and Sh400 million on a device management system that will help us closely monitor mobile phones and the activities around them."

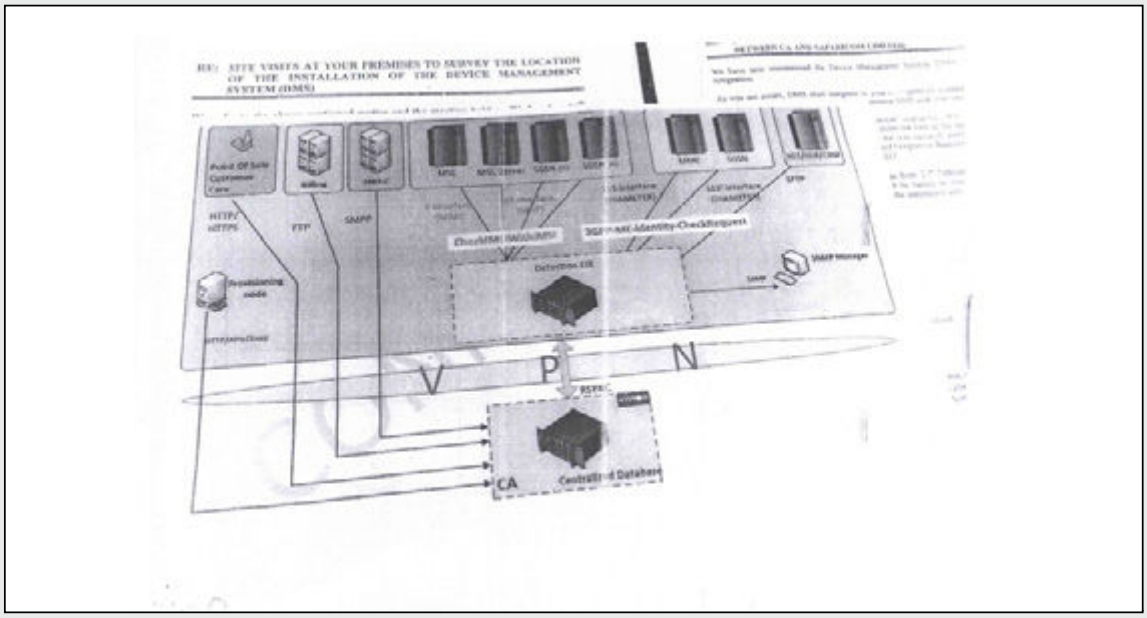
65 Email to Kenya ICT Association mailing list, 14 January 2017, available at: https://www.kictanet.or.ke/?p=26906

66 Christopher Wambua of the CA stated in an email to the Kenya ICT Action Network: "None of the equipment cited are meant to closely monitor mobile phones. The Spectrum Management and Monitoring System is meant to manage frequency spectrum resources including planning, assignment and monitoring to ensure compliance with the license parameters. On the other hand, the device management system is meant to deactivate all counterfeit mobile devices imported into the country illegally in order to ensure the phones are not used for criminal purposes." 14 January 2017, available at: https://www.kictanet.or.ke/?p=26909

67 "Big Brother could start tapping your calls, texts from next week," Daily Nation, 17 February 2017, available at: http://www.nation.co.ke/news/Government-likely-to-start-phone-tapping/1056-3816372-m5vnfx/index.html

a communications surveillance program, which CA denied on technical grounds.[68] The system was designed to deny service to "illegal communications devices" including counterfeit, substandard, non-type approved and stolen devices, according to the CA.[69] The system requires access to Kenyans' call data records (CDRs) or home location records (HLRs). The CA's 31 January letter to Safaricom states that the CA's contractor in charge of the device management system required "access [to] information on the IMEI, IMSI, MSISDN and CDRs of subscribers on your [Safaricom's] network."[70]

CA Director of Licensing Compliance and Standards Chris Kemei stated to Privacy International that analysis of CDR data is necessary to establish broad patterns of traffic which may indicate illegal activity such as SIM boxing, "but only in cases where there is that suspicion…we can use that system to confirm whether that is the case or not".



The device management system proposed by the Communications Authority (CA) would connect databases of several network operators to a centralized database under CA control. This information would include call data records (CDR) and home location records (HLR), a database of permanent subscriber information.

Credit: January 2017. Obtained by Privacy International.

68 Email to Kenya ICT Association mailing list from Christopher Wambua, Ag. Director Consumer and Public Affairs, Communications Authority, 17 February 2017, available at: https://lists.kictanet.or.ke/pipermail/kictanet/2017-February/051092.html

69 "Authority Refutes Misleading Media reports on Device Management System (DMS)", Communications Authority of Kenya, 17 February 2017, available at: http://www.ca.go.ke/index.php/what-we-do/94-news/425-authority-refutes-misleading-media-reports-on-device-management-system

70 On file with Privacy International.

Social media monitoring

A social media monitoring project also gives further reason to be concerned by the CA's plans. In late 2016, the CA finalized a contract with Israeli 'web intelligence' firm webintPro,[71] according to CA sources. The firm's HIWIRE technology allows for the capture and analysis of open-source traffic, and is particularly adapted to analyzing social media.[72] Some of the features of the system include the ability to map links between social media users, 'real time' surveillance of target objects, presumably individual users. Its virtual HUMINT (human intelligence) platform allows for analysts to proactively engage users online, "switch[ing] identities instantly" for "cloaked target engagement".[73] WebintPro did not respond to Privacy International requests for comment.

The past few months have seen claims[74] and counter-claims of fraud and intimidation in the election-planning process. Will surveillance facilitate this dynamic and if so, to what extent?

'Acceptable deaths'

Reflecting about the election, current and former NIS officers admitted to personally witnessing the misuse of communications surveillance powers. But they saw these incursions as justifiable. "It is what you might call 'acceptable deaths.'… People will accept it, or it will have a waiver to a certain extent," explained one. "We can infringe into your rights because of saving the lives of a hundred Kenyans…Not that we like doing it," stated another.

There are real doubts as to whether Kenya's limited intelligence oversight mechanisms are equipped to detect and rectify law enforcement and intelligence agents' abuses of communications surveillance powers. The CA oversees the telecommunications industry and is mandated to inspect all interception equipment in the country. However, the CA has little if any knowledge of the actual use of

71 Privacy International was not able to confirm that the webintPro contract corresponds exactly to the social media monitoring initiative announced by the CA in January 2017. Yet webintPro's technology would be most suited to the social media monitoring initiative, out of the three announced projects.

72 webintPro Web Intelligence Systems, 2017, available at: http://www.webintpro.com

73 webintPro Web Intelligence Systems, 2017, available at: http://www.webintpro.com

74 See for example: "UN experts urge Kenya to end crackdown on rights groups to ensure fair elections", United Nations Office of the High Commissioner for Human Rights, 14 February 2017, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21172&LangID=E and "Cord claims of Jubilee plot to rig 2017 General Election," The Daily Nation, 16 November 2016, available at: http://www.nation.co.ke/news/politics/Cord-claims-of-Jubilee-plot-to-rig-2017-General-Election/1064-3453518-d98twwz/

the interception equipment in place. Intelligence agents generally dismissed the agency as "just civilians," while a Communications Authority official called the NIS and CA's relationship "very cordial," though only a small number of CA officials would have detailed knowledge of communications interception architecture.[75] Christopher Wambua, Acting Director of Consumer and Public Affairs denied that the Communications Authority has particular knowledge of communications surveillance in Kenya, stating: "If there is any surveillance that is done, it is done by the law enforcement and we are not involved".

The Independent Policing Oversight Authority, whose mandate is limited to reviewing police[76] and not military or intelligence agency activities, struggles to do its job in face of intimidation.[77] Very little, if any, action has been taken by the Intelligence and Security Committee or the Intelligence Service Complaints Board Oversight to address such excesses.

The pressure on telecommunications providers to provide information, both with and without warrants, as well as the vagueness and laxity in existing communications surveillance laws, make it unlikely that surveillance practices will be reported and scrutinized.

75 The development of Kenya's cybersecurity infrastructure is the focus of a forthcoming Privacy International investigation.

76 "IPOA Profile", Independent Policing Oversight Authority, 2017, available at: http://www.ipoa.go.ke/ipoa-profile/

77 "IPOA embarrass and intimidate police officers, says Interior PS Karanja Kibicho," The Standard, 14 December 2016, available at: https://www.standardmedia.co.ke/article/2000226807/ipoa-embarrass-and-intimidate-police-officers-says-interior-ps-karanja-

Recommendations

To the Independent Policing Oversight Authority

- Begin an investigation into the practice of police officers receiving intelligence from National Intelligence Service officers, in breach of s. 49(4) of the National Police Service Act of 2011.

- Investigate the role communications surveillance plays in the already established practice of torture, cruel, inhuman, degrading treatment and other serious human rights violations.

To the Kenya National Commission on Human Rights

- Investigate, in line with section 30 of the National Intelligence Services Act, in its official capacity under s. 59 of the Constitution of Kenya, the National Intelligence Service for the illegal interception of communications.

To The Government of Kenya

- Reform legislation governing communications surveillance which facilitates Direct Access to communication networks, in particular, s.31 of the Kenya Information and Communications Act.

- Clarify to telecommunication operators their freedom to produce transparency reports on requests from communications and remove any restrictions currently in place that prevent disclosure by telecommunication operators of aggregated statistics of requests for communications data.

To the Inspector-General of The National Police of Kenya

- In line with your functions under s. 10 of the National Police Service Act, audit the police operations involving improperly obtained communications surveillance.

- Cooperate with any investigation carried out by the Independent Police Oversight Authority and implement the decisions of such investigation.

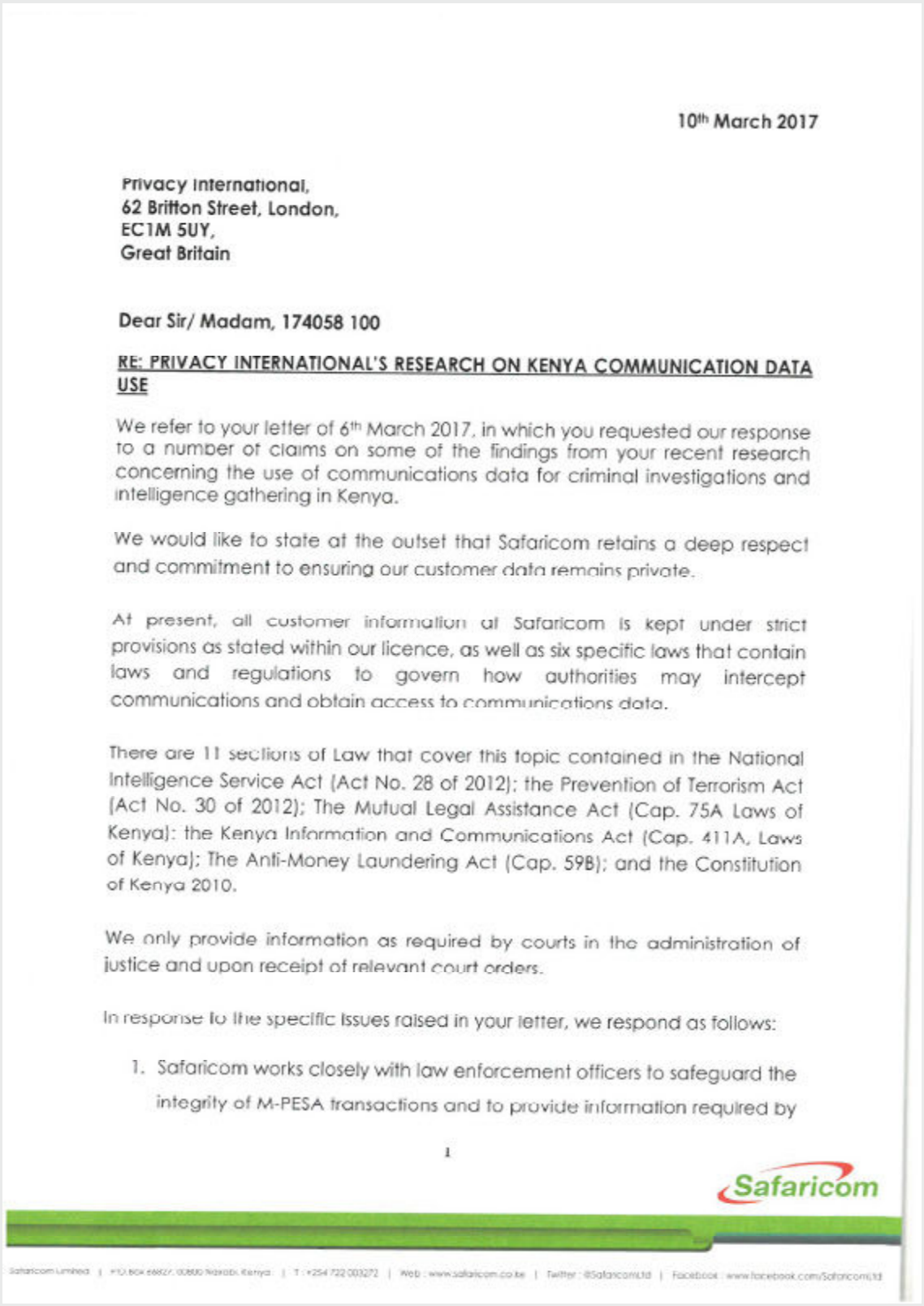
To the Cabinet Secretary

- Release the yearly reports, prepared under s. 28 of the National Intelligence Service Act (2012), and detail any conclusions and recommendations made during these inspections.

To the National Security Council

- Investigate, under s. 29 of the National Intelligence Services Act (2012), the direct and indirect violations of human rights by agents, in line with s. 59(2)(d) of the Kenyan Constitution.

Annex 1: Response from Safaricom



10th March 2017

Privacy International,
62 Britton Street, London,
EC1M 5UY,
Great Britain

Dear Sir/ Madam, 174058 100

RE: PRIVACY INTERNATIONAL'S RESEARCH ON KENYA COMMUNICATION DATA USE

We refer to your letter of 6th March 2017, in which you requested our response to a number of claims on some of the findings from your recent research concerning the use of communications data for criminal investigations and intelligence gathering in Kenya.

We would like to state at the outset that Safaricom retains a deep respect and commitment to ensuring our customer data remains private.

At present, all customer information at Safaricom is kept under strict provisions as stated within our licence, as well as six specific laws that contain laws and regulations to govern how authorities may intercept communications and obtain access to communications data.

There are 11 sections of Law that cover this topic contained in the National Intelligence Service Act (Act No. 28 of 2012); the Prevention of Terrorism Act (Act No. 30 of 2012); The Mutual Legal Assistance Act (Cap. 75A Laws of Kenya); the Kenya Information and Communications Act (Cap. 411A, Laws of Kenya); The Anti-Money Laundering Act (Cap. 59B); and the Constitution of Kenya 2010.

We only provide information as required by courts in the administration of justice and upon receipt of relevant court orders.

In response to the specific issues raised in your letter, we respond as follows:

1. Safaricom works closely with law enforcement officers to safeguard the integrity of M-PESA transactions and to provide information required by

1

Safaricom

Safaricom Limited | P.O. Box 66827, 00800 Nairobi, Kenya | T: +254 722 003272 | Web: www.safaricom.co.ke | Twitter: @SafaricomLtd | Facebook: www.facebook.com/SafaricomLtd

Annex 1: Response from Safaricom page 2

courts in the administration of justice. The Criminal Investigations Directorate has designated officers who collect such information from our offices. We do not have a specific office space for the law enforcement officers.

2. Safaricom has a fully fledged Ethics and Compliance department, comprising of Safaricom Staff, whose mandate is as follows:-
   - Internal fraud management (including Fraud prevention, detection and investigations).
   - Fraud Management for Customer and Business Partners.
   - Promoting good business ethics across the organization.
   - Reviewing and ensuring the company complies with the relevant laws and regulations.
3. Safaricom does not have a "fraud database". However, as required by law, authorised staff have access to systems and tools to verify customer identity information (KYC), which is a pre-requisite to offering any of our services to customers.
4. No. Only authorised Safaricom staff have access to systems and tools that can access confidential customer information and this access is controlled and monitored.
5. This is typical information for most call data records.
6. This claim is not true.
7. This claim is not true.

In response to two points you forwarded for clarity, we would like to state that we have no relationship with NIS as relates to communication surveillance in Kenya; and we do not have any officers or other representatives of the NIS who are employed, formally or informally, at Safaricom.

We believe that customers have a fundamental right to privacy, which is enshrined in international human rights law and standards. Ensuring that right is respected is one of our highest priorities. It is also an integral part of the

2

Safaricom

Annex 1: Response from Safaricom page 3



Safaricom Code of Conduct, a document that everyone who works for us has to follow at all times.

I trust that this answers the queries raised in your letter. We are happy to assist should you need more clarification.

Yours faithfully,

Bob Collymore
CEO, Safaricom Limited

cc: Stephen Chege, Director – Corporate Affairs, Safaricom

3

Safaricom

Safaricom Limited | P.O.Box 66827, 00800 Nairobi, Kenya. | T: +254 722 003272 | Web: www.safaricom.co.ke | Twitter: @SafaricomLtd | Facebook: www.facebook.com/SafaricomLtd

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471