Telecoms, Ubiquitous Surveillance and State Crime

A Case Study From Kenya

Namir Shabibi
Independent
Investigative
Journalist

DISRUPTION
NETWORK
INSTITUTE

THEKILL
.CLOUD

Director & Editor: Tatiana Bazzichelli

Creative Producer & Layout: Jonas Frankki

Additional Research: Sindre Kjaereng,
University of Westminster Alumnus

Peer Reviewer: Ernest Cornel Oduor,
Senior Communications Officer, Kenya Human Rights Commission

Copy Editing: Etienne Darcas

Proofreading: Lina Abazine, Tatiana Bazzichelli, Giulia Vitali

Advisory Board:
Heba Y. Amin, Khalil Dewan, Anthony Downey, Thomas Drake,
Jennifer Gibson, Alexa Koenig, Matthias Monroy, Jesselyn
Radack, Andreas Schüller, Rima Sghaier

Advisory Fellows:
Naomi Colvin, Lisa Ling, Joana Moll, Jack Poulson

Social Media: Savannah Garcia

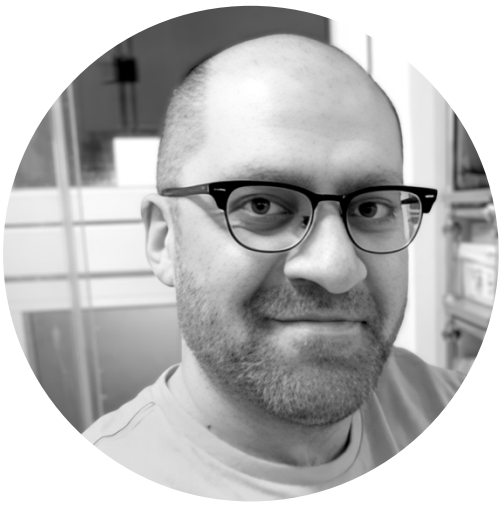
Administration: Sophia Schmidt

Disruption Network Institute
disruption.institute

Disruption Network Institute is a project
of Disruption Network Lab e. V.
disruptionlab.org

The fellowship programme 2025–2026 has been
made possible with support from Luminate.

Publishing Partner: Kenya Human Rights Commission (KHRC)



Namir Shabibi

Independent Investigative Journalist, UK

Namir Shabibi is an independent investigative journalist working at the intersection of tech and state crime. He is a visiting lecturer in Geopolitics, and a Quintin Hogg-sponsored PhD candidate researching covert intelligence operations in global majority countries. Namir also leads the Working Group on Telecoms, Spyware and Surveillance, based at the University of Westminster, and conducts research for Unredacted, a national security investigative project. Namir is a former International Committee of the Red Cross delegate investigating breaches of the Geneva Conventions in Darfur and Guantanamo Bay.

Telecoms, Ubiquitous Surveillance and State Crime: A Case Study from Kenya

Namir Shabibi

Contents

Acronyms 5

1. Introduction 6
    - Approach 8
2. Mobile Networks in Digital Public Life 9
    - Ubiquitous Technical Surveillance 11
    - Mobile Networks as Digital Public Infrastructure 13
    - Ubiquitous Data Collection and Mobile Networks 14
    - A Tightening Web of Surveillance 15
3. The Militarisation of Surveillance in Telecoms Networks 16
    - Link Analysis 19
    - Border Monitoring 20
    - Proximity Alarms 20
    - Historic Tracking and Live Tracing 20
4. The Intersection of Militarised Tech and State Crime in Kenya 21
    - State Crime in Kenya 21
    - Telecoms and Policing as an Integrated Operation 22
    - 'Small Wars, Big Data' 24
    - Big Tech, Big Data and State-Corporate Crime 26
5. Conclusion 29
6. Bibliography 31

Acronyms

ATPU	Anti-Terrorism Police Unit (Kenya), which is part of Kenya's DCI
BTS	Base Transceiver Station, otherwise known as a phone mast or base station
CDR	Call Data Record
COIN	Counterinsurgency
DCI	Directorate of Criminal Investigations (Kenya)
DEA	Drug Enforcement Administration (USA)
DPI	Digital Public Infrastructure
GCHQ	Government Communications Headquarters (UK)
GNSS	Global Navigation Satellite System, which provides GPS data
HRD	Human Rights Defender
ICT	Information and Communications Technology
IMEI	International Mobile Equipment Identity number (i.e. the phone's serial code)
IMSI	International Mobile Subscriber Identity number (i.e. the sim card serial code)
LELO	Law Enforcement Liaison Office (an office of Kenyan MNO, Safaricom PLC)
MNO	Mobile Network Operator
MSISDN	Mobile Station International Subscriber Directory Number (i.e. the mobile phone number)
NIS	National Intelligence Service (Kenya)
NSA	National Security Agency (USA)
UTI	Ubiquitous Technical Intelligence
UTS	Ubiquitous Technical Surveillance

1. Introduction

In the past half decade, civil society organisations have dedicated the bulk of their resources on mobile phone surveillance towards a niche area – spyware use – despite its application being extremely rare. As a consequence, human rights organisations in particular have developed a blind spot towards the advancement of telecoms networks, their role in 'ubiquitous technical surveillance' and the actual (rather than supposed) modus operandi of state crime in the Majority World. When considering the integration of telecoms networks into digital public infrastructure, as well as advances in the user geolocation capabilities of those networks, and the increased use of military intelligence tech within them, a disturbing picture emerges; that of the grave vulnerability of citizen-subjects to what the US Supreme Court described as "near-perfect surveillance" (Wessler, 2019).

From this surveillance vector, there is no 'opting-out' – bar exiting digital public services, mobile banking and mobile digital life more broadly. And it is this site that transnational corporations and the state, from the relatively democratic to the downright authoritarian, have consistently exploited, with insufficient opposition and antagonism from an international human rights community. Regrettably, this community's focus has been redirected by a tech infatuation with documenting rare, highly-specialised malware infiltrations of individual phones, and playing technological cat-and-mouse with its makers and their spyware. Consequently, precious human rights, investigative journalistic and legal resources have been misdirected away from efforts to document, expose and challenge mass technologies of control and harm, despite their centrality to the modus operandi of targeting, state crime and life-and-death outcomes in the Global Majority.

The aims of this research paper are threefold: 1) To situate the gross overrepresentation of spyware, and underrepresentation of other mobile surveillance techniques by pointing to the centrality of mobile telecoms networks in digital public infrastructure, rendering it a ubiquitous sensor from which so much technical intelligence is derived; 2) To draw the reader's attention to the combination of advancements in mobile location intelligence techniques, with exponential developments in accuracy and frequency of location logging, and to demonstrate the systematic 'transference' of military-intelligence analytics tools to everyday policing and law enforcement, augmented by machine-learning algorithms, and finally; 3) To apprise the reader of the centrality of mobile networks and their relevant technologies to the surveillance and targeting of vulnerable communities, particularly migrant and border communities, with life-or-death outcomes. Throughout, this paper will refer to the author's published and unpublished investigative journalism in Kenya, with references to documented cases elsewhere.

This paper begins by articulating the transformation of mobile telecoms into digital public infrastructure, especially given its necessity to access services for 'unbanked' populations. It then explains how mobiles routinely generate cell site data, from which there is no opting out, which enable historic surveillance and live location intelligence or 'tracing'. Given their ubiquitous use, it follows that mobile networks are a key node in what the so-called 'intelligence community' refers to as ubiquitous technical surveillance. As an elite option, spyware is not only used extremely rarely but is also simply unnecessary for most targets. Indeed, many of spyware's purposes can be achieved without use of costly malware, using a combination of cell site surveillance, 'lawful intercept', IMSI catchers, and forensic imaging and extraction, amongst other techniques.

This research paper continues by charting the development of 2G networks to 5G and 6G, and the exponential advances in geolocation of handsets, link analysis and other forms of network investigations. 6G threatens to extend dystopian advances in location intelligence and sensing accuracy. These technological developments should also be considered along with the growing number of cell towers and cells themselves, to meet network advances, which serve to further tighten the weave and accuracy of the surveillance web. Once mobile telecoms are appreciated as an essential tool in access to digital public infrastructure, not to mention modern social life, it follows that it is a ubiquitous data collector whose precision and invasiveness is only growing. From there, the state's reliance on it as the go-to site of analysis and exploitation becomes apparent.

The next section points to the proliferation of militarised tech that allows for the predictive identification of suspects, pre-crime modelling of communities and the predictive linking of individuals to suspects. Over more than a decade, machine-learning algorithms have also been employed to do the above at pace. What were once the reserve of only the best-resourced signals intelligence agencies, such as GCHQ and the NSA, are now commonly applied by ICT firms against MNO data for police and other state security benefit. These technologies enable the militarisation of surveillance, in that they view entire communities or geographies as suspect or threatening, thus justifying bulk, predictive and targeted interventions. And, as always, it is the marginalised regions where vulnerable migrants and border populations are subjected to the most invasive forms of blanket, geo-fenced, predictive surveillance.

This paper concludes with a case study centred around the author's recent investigative journalism and ethnography in Kenya, which exemplifies the centrality of mobile telecoms to digital public life, while doubling up as a danger to the majority. The case study will summarise Kenya's contemporary history of state criminality, and how near-monopoly telecoms operator Safaricom integrated police into its daily operations and services, which constitute digital public infrastructure. It

shows, with source interviews and other data, how Safaricom sought to integrate police into its operations, to streamline targeted surveillance and investigations, and how it tasked Britain's Neural Technologies to make it happen. The Safaricom-police integrated operation then transformed from one of targeted surveillance to include bulk spying with predictive algorithms. As such, it constitutes one of many examples of the transference of military intelligence tech and practice. Relying on field research by the author, the case study also cites testimony from Kenyan state security officers on how they utilise that data in the targeting cycle. These invasive surveillance practices are not merely matters of privacy, as they are so often framed by the human rights community: To many Kenyans, especially the dissident and marginalised, these are life-or-death questions. It concludes by showing how police and Safaricom exploit ubiquitous data collection for surveillance and targeting, while frustrating those investigating enforced disappearances, who could equally utilise the telecoms (cell site) data to help solve state crime.

The advances in telecoms networks, their ubiquitous use and exploitation, and the militarised use of tech applied to them, have brought us to a scenario once imagined in nightmares: every connected mobile phone is now an effective ankle tag constituting the authoritarian state's dream-come-true. Though the landscape remains bleak, this paper concludes on a positive note, offering reflections on counter-measures that activists, dissidents and other targets of state crime can take, and how the very tech that is weaponised against them can be flipped and used in the investigation of state crime – particularly enforced disappearance.

Approach

A note on the unorthodox nature of this paper is warranted. While the author is both a journalist and scholar, this piece of work belongs in neither camp. Instead, it is a hybrid between longform journalism and normative argumentation, with the trappings of academic referencing. The paper's purpose is not to comprehensively argue a single, overarching point, but to connect various strands that are often treated in isolation, in order to make provocative arguments for discussion. Take, for example, digital public infrastructure and state crime. Seldom do the two fields of study meet. On the other hand, 'ubiquitous technical surveillance' was conceived by the intelligence community to reckon with counter-intelligence in an age of ubiquitous technical surveillance. Yet its mention in journalism, or by NGOs, is rare, despite its applicability to all when discussing human rights, and particularly counter-surveillance measures. Similarly, the concept of 'small wars', Big Data and Big Tech are all-too-often siloed from the issues and practices they intersect with. So, while this paper's aim is to connect these concepts to provoke discussion, space constraints mean that they were done without each concept or connection being fully elucidated or explored.

Insofar as this paper may be considered longform journalism, it is based on all-source methods of research and investigation conducted by the author under various guises: originally as an investigator for a human rights NGO, then as a documentary producer, later as an investigative journalist, and more recently as an adviser to public-interest advocacy groups. Clandestine and secretive practices and systems such as those described in this paper often necessitate human source cultivation for their thorough research. As such, the main method in this paper is gumshoe investigative reporting, undertaken in Kenya, the UK and the US since 2016 – primarily as an independent journalist. The interviews were conducted principally with both the protagonists concerned – i.e. intelligence officers, police and paramilitaries – but also with the affected communities, namely the victims of state crime, including enforced disappearance. If a label must be applied to the interview methods, they were what the academy terms 'investigative ethnography', with only lightly structured interviews. This paper also cites documents leaked to the author, from officers within Kenyan security agencies, as well as sources within the telecoms industry. Publications from the author's relevant journalism are cited within. However, much remains to be published – in due course.

2. Mobile Networks in Digital Public Life

In the past decade, human rights organisations as well as investigative journalists have dedicated significant resources on mobile digital surveillance towards research, documentation and investigation of corporate mobile cyber intrusion capabilities, better known as corporate 'mobile spyware'. Whether causative or symptomatic of this focus, in parallel the funding of civil society research and litigation in the state surveillance domain is almost overwhelmingly focused on corporate mobile spyware, at the cost of other forms of mobile and digital surveillance. However, those who holistically study, work to counter, or participate in state surveillance practices will readily explain that commercial spyware's use is "extremely rare" and "designed for the very few individuals who, because of who they are or what they do" (*About Lockdown Mode*, 2026). In short, mobile spyware's primary benefit is the clandestine exfiltration of data, and live monitoring of targets whose mobile tech, applications (e.g. Signal) or counter-surveillance practice necessitate surveillance from within the device. This tech is applied to an extremely small sliver of targets of state investigations and repression in the majority world. Despite this, human rights organisations have gone as far as to claim that mobile spyware is

> *one of the most pressing threats* to democracy, fundamental rights, and cybersecurity in the European Union and globally[1] (*Spyware and State Abuse: The Case for an EU-Wide Ban*, 2025)

The disparity between civil society focus and actual surveillance practices derives, in part, from the stipulations of major funders. In recent years, the bulk of civil society funding for state surveillance research and investigation has been dedicated to commercial mobile spyware (henceforth: 'spyware') – to the exclusion of other forms of mobile and other surveillance (*Spyware Accountability Initiative*, 2024). Adding to the absurdity of it all, the US State Department has provided significant support to counter the commercial proliferation of spyware (*New U.S.-led Actions*, 2024). Yet these initiatives are seldom interrogated as to why the diplomatic arm of a government that is itself so implicated in producing spyware and hacking devices – principally through the National Security Agency – would position itself as publicly as opposed to *commercial* proliferation. One clue can be found in the US government's alarm at the discovery in 2021 that Israeli Pegasus spyware was used against the iPhones of 11 of its own officials in Uganda.[2] Yet no such alarm was expressed when, six years earlier, the Ugandan government – a US government ally – was found to have deployed spyware against domestic opposition leaders and the media (Lauterbach, 2015).

Notwithstanding the above, the issues with this misdirection of focus, and resources, towards spyware are four-fold, among others: first, it exhibits a problematic ignorance of the broader ecosystem of state surveillance, the capabilities that exist within them, and the priority that the state affords to certain tools over others. The spyware focus misdirects attention away from more ubiquitous forms of state surveillance that enables the exercise of abusive state power, leaving those practices largely ignored or insufficiently challenged. While spyware's operators primarily use it for the *clandestine collection* of intelligence on higher value targets (and by-extension their networks), its use remains expensive, highly specialised and target-specific. Much but not all of what spyware achieves can be realised through network-level telecoms surveillance, along with other tools, and often at little-to-no cost.

Second, as the author has experienced, the laser focus on spyware results in counter-surveillance advice tailored specifically towards it for human rights defenders and other vulnerable people. One human rights campaigner recently

[1] Emphasis added.

[2] For more on the Uganda spyware case, see Benner, Sanger and Barnes, 2021. In response to it, then-President Biden planned a crackdown on the use of such software at a White House summit, to which he has invited dozens of countries — including Israel, whose 'former' intelligence officials were involved in Pegasus' development. For more on Pegasus' development, see Bergman and Mazetti, 2022.

complained to the author that human rights defenders (HRDs) had declined to use Apple's 'lockdown mode' (a counter-spyware measure) as too burdensome and restrictive of their mobile use. As a consequence, HRDs have resorted to using 'dumb phones' as 'burner phones' to counter mobile surveillance, since their civil society advisers had failed to explain (or were simply unaware) that location tracking, link analysis and user identification, not to mention 'lawful intercept' of call and SMS content, were all achievable through the telecoms network itself and require no spyware infection. And should the state seize the target HRD's phone, almost all of what can be achieved using spyware is possible through the use of forensic extraction devices. Finally, another consequence of the disproportionate focus on spyware is that telecoms networks as a site of surveillance has been taken for granted by civil society. That is to say that the technological advancement of those networks, as well as growth of their infrastructure, has largely been ignored – despite those advancements from the 1990s rendering mobile surveillance exponentially more accurate.

Due to space constraints, the following section will focus on three areas that civil society's focus on spyware has neglected, as groundwork for a case study of state-corporate surveillance in the majority world. The first point to be made is that the study of state surveillance practice should be inextricably bound to the concept of ubiquitous technical intelligence and surveillance. Without acknowledging the ubiquity of certain sensors, and the surveillance threats they pose, the go-to methods of state spying are bound to be lost on researchers and campaigners. Certainly, the intelligence community is alive to these surveillance threats, resulting in extended discussion around the difficulty of counter-surveillance in an age of ubiquitous technical surveillance (UTS). The second is that the rise of digital public infrastructure (DPI), and citizen reliance on it, particularly mobile phones, renders it a vector for ubiquitous surveillance. One must therefore consider the role of mobile network operators (MNOs) within the ecosystem of DPI to appreciate both their ubiquity, and thus their vulnerability to state-corporate surveillance. And finally, to understand the surveillance threat posed by telecoms networks, advancements in location data frequency and accuracy should be recognised. Far from the inaccuracy of 2G networks, today's 5G networks, the proliferation of masts and cells, the storage of historic use data, as well as new ways of determining a mobile handset's location (known as location intelligence) allow for increasingly accurate surveillance. And those capabilities are all inherent to the network.

Ubiquitous Technical Surveillance

The US Federal Bureau of Investigation defines UTS as "the widespread collection of data and analytic methodologies for the purpose of connecting people to things, events, or locations" ('Protecting U.S. National Security', 2025, p. 9). The sources

and methods through which UTS is achieved are too many to list here. Some data collection sources are obvious; social media activity, phone use and CCTV networks being among them. Less apparent is other data sources, such as satellite imagery, mobile ad ID tracking, mobile signal message logs; with which the aforementioned data sets are also fused. UTS is described in terms of five data-collection pathways, also referred to as the five UTS Threat Vectors:

(i) Online UTS in which every interaction creates a unique digital footprint and allows for an inference of an individual's location, identity, interests, and behaviour patterns.

(ii) Electronic UTS arises from the signals emitted by connected devices such as Wi-Fi, cellular networks, Bluetooth, GPS and Internet of Things systems.

(iii) Visual-Physical UTS consists of camera-based surveillance in physical spaces, including CCTV, smart doorbells, and facial recognition.

(iv) Financial UTS is generated through everyday transactions such as card payments, mobile banking and money transfers. This creates financial trails that enable behavioural analysis.

(v) Travel UTS encompasses data produced by mobility, including flight bookings, GPS navigation and digital coordination with travel companions (Adekunte, Sadiku and Sadiku, 2024, p. 232)

As one US Army op-ed explains, the "constant monitoring" of UTS "allows for the long-term storage and analysis of information, potentially reconstructing past events indefinitely" (Bell, 2025). The threat that this poses to human intelligence operations should be readily apparent. It follows therefore that sections of the CIA have described UTS as an "existential" surveillance threat to its officers, agents and assets. In 2022, then-CIA director William Burns explained that UTS "means that intelligence officers are being watched, tracked, and observed all the time. (...) [T]his has prompted us to fundamentally rethink how we do our operations" (Burns, 2022, p. 6).

An example of UTS posing a counter-intelligence threat to US military forces and their secrecy is recognisable from the Strava 'leaks', when the fitness tracking app indirectly gave away the location of secret US army bases, through publication of user exercise routes (Hern, 2018). Issues around Strava continue: this year, hundreds of exercise routes of UK force personnel were exposed (Holmes, 2026). Other location-based apps such as Tinder have been found to expose similar vulnerabilities (Wolfgang, 2026). While some writers have framed the Strava leaks in terms of the threat posed by UTS, it is important to recognise that the user of Strava is

not strictly necessary (Sherman, 2025). Whereas basic telecoms network services (calls, data, SMS) are increasingly essential to access digital public infrastructure and social life more broadly, Strava remains an optional nicety, essential neither to exercise nor social connection. Thus, one can choose to opt out of Strava, or Tinder, with no serious consequence for access to public services and digital social life. This underscores the need to refocus discussion around ubiquitous surveillance on the more invisible technologies that have been taken for granted and are an inextricable part of our lives.

Among others, three developments have helped render surveillance ubiquitous: over the years, the costs associated with surveillance data storage have decreased, allowing more data to be stored at less cost, constituting a boon for corporate surveillance capitalism (Sanchez, 2020, p. 83). Second, personal digital devices and wearable technologies have proliferated, and tracking technology has been integrated into transport among other infrastructures, such that more aspects of public life have become trackable and tracked. And finally, the notion of mass state monitoring and surveillance has become more socially acceptable, especially due to the Covid-19 pandemic, when it was employed to control the spread of the virus (Sanchez, 2020, p. 2).

Mobile Networks as Digital Public Infrastructure

Digital public infrastructure (DPI) has been described as an approach "to building society-scale digital systems that can boost economic opportunities and enable better public services" (Wilkinson, Krasodomski and Wilkinson, 2025, p. 7). Its nominal aim is to drive sustainable development, with modern societies increasingly reliant on DPI to provide essential services such as identity verification, payments, and sharing of data. While DPI project approaches are supposed to lead with public sector standards, private sector initiatives have been known to become national de facto standard. One such case is in Kenya, when in 2007 mobile network operator Safaricom PLC launched the mobile money system M-Pesa, which became the de facto standard for digital payments in Kenya, such that it monopolised the market (Sankritik and Shetty, 2025, p. 10). Interoperability between M-Pesa and bank accounts only later followed and, as such, M-Pesa became DPI. Today, M-Pesa is the largest mobile money system and covers merchant payments (Lipa Na M-PESA), micro loans and savings (M-Shwari), Kenya Central Bank savings and loans (KCB M-Pesa) and medical 'rainy day' funds (M-TIBA), among others. While some Kenyan government online services advertise multiple payment methods, in reality some can only be paid for using M-Pesa, making its use obligatory for Kenyans. Some

Kenyan public services have only accepted M-Pesa as a form of payment.[3] Safaricom, which now describes itself as a "purpose-led tech company" is central to Kenyan infrastructure in manifold other ways (*Safaricom | What We Do*, no date). It operates city-wide surveillance CCTV networks, home and business internet, and digital solutions for smallholders (Digi Farm). As East Africa's most profitable tech company (Thomas, 2026), by 2030 Safaricom aims to become the continent's biggest (*Safaricom | What We Do*, no date).

Ubiquitous Data Collection and Mobile Networks

As standard practice, mobile network operators (MNOs) also log the metadata of all calls (sent and received), SMS and internet data connections. These are known as 'events', which are stored as data logs and are collectively known as Call Data Records.[4] CDRs stored on MNO databases are logs of all incoming and outgoing CDR events. Each event log comprises the subscriber phone number (MSISDN), originating phone number (A), the recipient phone number (B), time and date, the type of event (call, SMS, data connection), then cell tower (or base transceiver station, BTS) connected to at the start and end of the call, the phone serial number (IMEI), the sim serial number (IMSI) and the ID name/number of the subscriber. Event logs can also include details of the directional cell (azimuth) to which the phone connected to at a given tower, depending on whether the MNO logs those details as well. Some MNOs also log 'timing advance' data with each event, which is a measurement of time a signal takes to reach the cell/base station from a mobile phone. Timing advance therefore allows for the rough estimation of a phone's location within a given cell sector. Going even further, a handful of MNOs also log signalling messages, which are administrative contacts between the phone and the network, such as when a phone is powered up/down and handed between masts. Those administrative contacts do not require active use of the phone, and are logged as location data points, generating far more location data points than a standard CDR dataset.

As historic records, generated near-contemporaneously, and stored for years, CDRs are immensely valuable to police investigators, from the identification of suspects to their tracking, and for use as an alibi in prosecutions. For example, an investigations and prosecutions manual written by the British Foreign Office for Kenya's Anti-Terrorism Police Unit (ATPU), which was leaked to the author, lists call and SMS data as "critical evidence" to seek in 13 of 37 categories of offences under terrorism, organised crime and firearms legislation. The invasive, historic

[3] The Likoni Channel ferry crossing's stipulation that only Safaricom's M-pesa could be used as payment is a case in point (Muyanga, 2021).

[4] In the United States they are known as Call Detail Records.

surveillance capability of CDR searches (known formally as 'cell site investigation') was not lost on the US Supreme Court, when in its decision concerning *Carpenter v. U.S.*, it argued that

> when the Government tracks the location of a cell phone it achieves *near perfect surveillance*, as if it had attached an ankle monitor to the phone's user… Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations. (Wessler, 2018)

The searches of CDRs by state security agencies therefore constitutes one of the most invasive violations of the right to privacy. Yet it is not the full picture of inherent telecoms surveillance capabilities, since it does not account for 'live tracing' targets; or what is more commonly known as suspect tracking. The geolocation of targets through live tracing is far more accurate. Whereas CDR searches will offer a historical to near-contemporaneous location history, at best it will offer details of the cell tower connected to, the particular cell (typically covering a 120-degree angle), and in rarer cases timing advance data (allowing the rough estimation of the handset's location within a given cell coverage area or sector). By contrast, a live trace utilises triangulation across multiple masts and signal strength measurement. In certain cases, the network can also prompt the mobile handset's GPS chip to report its location, along with hotspot data.[5]

A Tightening Web of Surveillance

The accuracy of MNO live tracing grows by the year. This is due to multiple developments, including the increase in number of cells and masts, shorter ranges per cell (with each new generation) and technological developments with each cell. Each generation of mobile network cell, from 2G > 3G > 4G and so on, brings with it a shortening of the range, that is the distance that each cell will cover. While 2G's *effective* range extends to 10 miles, and 3G extends to 3 miles, the fastest 5G cells cover up to a 1/3 of a mile.[6] This means that for the deployment of 5G coverage, far more cells (and therefore cell towers) are needed to cover the same area than, say, 3G cells. This has a direct consequence on the accuracy of live tracking

[5] In the United States, it is a feature known as E911 ('Wireless Call Location Services: Tech Note', 2007).

[6] These are effective – not theoretical – ranges, and figures cited vary. Cell range is susceptible to topography, foliage and reflective (glass) buildings, among other things. The figures quoted here are intended as a guide, and to reflect the fact that each generation of covers shorter distances.

surveillance. However, some figures are needed to illustrate the problem. Take the UK, for example. As reported in 2018, there were around 35,000 cell sites (macro and micro) used by the mobile networks (Yardley *et al.*, 2018, p. 9). Today, that number is at least 78,000 ('Freedom of Information request reference 02164629', 2026), representing an increase of at least 100%, though the figure is likely to be significantly higher.[7] Not only does the increase in number of cells and towers represent greater coverage of the UK, but when a handset is within communicable distance of multiple, rather than one or two masts, it allows for more accurate geolocation of said handset, when conducting a 'live trace' on the number it carries.

Though already established in industrialised nations, as MNOs deploy 5G next-generation radio access networks (NG-RANs) in the Global Majority, accuracy will increase exponentially, with smaller cells and 'beamforming antennas' aiding the geolocation of connected handsets. Among other technological developments, the fusion of 5G and GNSS positioning means that in urban environments geolocation within 10 m accuracy can be achieved (Dwivedi *et al.*, 2020). However, it is the forthcoming generation (6G) that promises dystopian levels of geolocation accuracy. 6G will integrate multiple technologies, including ultra-broadband and machine-learning. This integration aims to enhance positioning accuracy exponentially and is projected to achieve an indoor positioning accuracy of 1 cm and outdoor positioning accuracy of 50 cm (Li, Fan and Wu, 2025, p. 11).

3. The Militarisation of Surveillance in Telecoms Networks

As we have seen, the ubiquitous if not inescapable use of mobile phones by the overwhelming majority of people across the globe is what renders them ubiquitous sensors, from which so much technical intelligence is derived by state security agencies, police and military forces – directly and indirectly. In the aftermath of Edward Snowden's revelations, much has been reported on the interception of mobile telecoms traffic by Anglo-American state security agencies, such as GCHQ and the NSA, *outside* of mobile network operator (MNO) control, though often with their acquiescence (MacAskill *et al.*, 2013). While some reporting has been dedicated to the incestuous relationship between MNOs and state security agencies, comparatively far less attention has been given, outside of the Anglo-European western context, to the relationship between those bodies in the majority world – even when the MNOs concerned are western corporate subsidiaries (Costa-Roberts, 2015).

[7] The number of 4G cell sites reported here gives an indication of the minimum, since it does not include 2G, 3G and 5G sites, though a single site may carry multiple cell generations.

Even less attention has been dedicated to the transference, over more than a decade, of military intelligence surveillance tech to domestic law enforcement for application against MNO data. That is the increasing application of machine-learning algorithms and predictive technologies to customer metadata at MNOs, with the purpose of generating risk intelligence and predicting criminality. With the bulk of migration-control activities taking place in the majority world, it behoves us as researchers concerned by the state of fundamental human rights to turn our attention to the technologies of surveillance and control there. This section now details those technologies, before turning to a case study from Kenya of how those technologies are applied to MNOs, and how they translate into paramilitary policing operations.

AI-augmented automated searching of MNO customer metadata by state security agencies, to establish patterns of life, link analysis, travel history and identify or predict criminality is far from new. Among its better-known earlier applications, the Snowden leaks showed the NSA applying machine-learning algorithms to MNO customer metadata to analyse behaviours and cross-validate with alleged 'known' Al-Qaeda couriers in Pakistan, as part of its SKYNET programme (Grothoff and Porup, 2016).[8] And while the NSA boasted that its preliminary results were "on the right track", it identified Al-Jazeera's Pakistan correspondent, Ahmad Zaidan as a "member of Al-Qaeda" after his phone exhibited travel history and links identified by the SKYNET algorithm as that of an Al-Qaeda courier (Currier, Greenwald and Fishman, 2015). From this, and the questionable, probabilistic science employed by the NSA, journalists asked:

> It's a small step from applying SKYNET logic to look for 'terrorists' in Pakistan to applying the same logic domestically to look for 'drug dealers' or 'protesters' or just people who disagree with the state. Killing people 'based on metadata,' as [General Michael] Hayden said, is easy to ignore when it happens far away in a foreign land. (Grothoff and Porup, 2016)

In fact, at the time the NSA slides – leaked by Snowden – were produced, that small step had already been taken years earlier, albeit without the aid of predictive algorithms. In Egypt, as protests raged at the spiralling price of bread flour in a generalised context of deprivation in March 2008, police requested that Vodafone Egypt geofence the area of the protest and hand over all details of all subscribers present – a process made simple by the country's mandatory sim registration (Espiner, 2009). From there it would have been easy and quick for Egyptian security services

[8] The NSA programme was based on an earlier US Drug Enforcement Administration (DEA) programme, which was used to track drug cartels' distribution networks in the USA, allowing agents to detect previously unknown trafficking rings and money handlers (Heath, 2015). Thanks to Jack Poulson for pointing out the connection and relevant reporting.

to identify all handsets (IMEIs) used with that sim (IMSI) or number (MSISDN) and vice-versa, conduct live traces on the users (thus revealing their live location), and perform social network link analysis, among others. Moreover, the identification of handsets operating within the geofence would have been broad, since only 2G and 3G cells were available in the country, meaning that historic searches of numbers active within the geofence would have collected numbers far outside of the site of the protest, due to the inaccuracy of geolocating handsets using 2G and 3G networks. Thus, the geofencing of the protest area will have identified many people unrelated to the protest. With Egyptian state security known for its brutal repression of protestors, including the systematic use of enforced disappearance, arbitrary detention, torture and summary execution, the identifying information handed over by Vodafone would have put the 22 mobile users arrested at grave risk (*Telco Hall of Shame: Vodafone*, 2013).

In the years following the NSA SKYNET leak by Snowden, similar if less sophisticated predictive algorithms were created by ICT companies, mostly but not exclusively from western countries, for use in the Global Majority. As mobile phones, 3G networks and mobile money transfer systems proliferated in the majority world, at times in lieu of public infrastructure development, the 2010s witnessed a burgeoning market for ICT companies dedicated to providing that analytic software to MNOs under the guise of 'fraud detection'. Undoubtedly, there are legitimate revenue-protection reasons for this kind of surveillance, such as fraud detection. However, as with all opportunities for bulk data analysis and prediction, it would soon be co-opted for state security purposes, with the MNOs and ICT companies being enthusiastic partners.

Here ICT companies and resource-starved state security agencies alike saw an opportunity to emulate GCHQ and NSA's programmes with similar software for the purposes of pre-crime analysis, criminal investigation, and investigating other subjects of interest, including dissidents, with the veneer of scientific rigour offered by algorithmic analysis. As a recent Airwars-AI Now analysis points out, the underlying 'random forest' method of algorithmic analysis – which was the basis of the NSA SKYNET programme – often produces false positives, leading to poor and unreliable performance: when applied to identify 'terror suspects' or 'combatants', random forests may mark an individual, like a journalist or humanitarian worker, as a 'militant' simply because they exhibit similar features as the categories they were trained on (Goodfriend *et al.*, 2026). Despite this, its use as a method of target identification from bulk datasets has expanded rapidly across the Global Majority MNOs. The logic being that the dataset is already captive; so why not exploit it? For state security agencies the world over, it has proven an opportunity too good to pass up.

In this context, this paper argues that the corporate technologies applied to MNOs have become 'militarised'. Traditional concepts of militarisation tend to focus on the paramilitarisation of tactical policing operations specifically, as well as their concomitant standard operating procedures, tactics, techniques and procedures, rules of engagement and weaponry (Kraska, 2007). Rather, this paper adopts recent arguments made by some human rights organisations; that militarisation of tech in civil and corporate infrastructure entails viewing entire territories or communities as threatening or potentially threatening (*Blurring the Line*, 2025). Thus the militarised approach to digital surveillance rationalises bulk collection, interception and analysis of mobile telecoms data against entire areas or nations. This is reflected in scholarship on counter-insurgency strategy, with "massed ISR" (intelligence, surveillance and reconnaissance) involving "persistent collection" being advocated as a central pillar of counter-insurgency (Flynn, Juergens and Cantrell, 2008, p. 58). It remains true that the likes of GCHQ and the NSA have long taken a militarised approach with bulk collection and predictive analysis of MNO data, even outside of conventional armed conflict and counter-insurgencies. This was seen clearly in the Snowden disclosures on GCHQ's TEMPORA programme (MacAskill *et al.*, 2013). However, the corporate sector has followed suit with the transference of military intelligence tech to digital public infrastructure. It can thus be argued that the corporate tech applied against MNO datasets has been militarised.

The following section details technologies applied against MNO data, either explicitly for migration control, or whether it logically follows that such technology could be used in this way. This is based on non-public and published sales brochures as well as source interviews conducted by the author in the course of their journalism (Shabibi, 2025).

Link Analysis

All operational mobile handsets can be geolocated within a particular area at any time – concurrently and retrospectively. This is because MNOs automatically log the location and other metadata around active uses of the network (CDRs), while some networks also log signalling messages, generated without any active use but simply when the phone is on. The storage of these data sets, at times for years by MNOs, provides the ability to locate all devices on network at any time – irrespective of whether the handset/user has previously been actively tracked or not (Betournay, 2026). The movement monitoring can be done in real time (automated or live trace), or as an historical analysis (CDR/signalling message analysis), to track a known target and/or identify potential associates of theirs. It can also be used to monitor the movements of other individual suspects, once they are identified. This dataset allows historic location investigation to be undertaken and identifies

behavioural relationships between mobile subscribers. None of this requires expensive spyware or other intrusive software, as the data is readily accessible to the MNO and state security agencies and searches conducted against them are not knowable by the target.

Border Monitoring

Algorithms are designed and applied to cell site data (CDRs, signalling message logs and live trace data) en-masse. But to put a specific area under surveillance requires 'geofencing' that area, since its national application would be too data-intensive. Geofencing is the placement of virtual boundaries drawn around a digital map to monitor activity within a given area, with automated systems of AI. As such, a geofence can be placed around a border region to monitor any and all activity within it. This enables security services to analyse all handsets crossing a border and from there gives them the ability to monitor their progress within all territories covered by national MNOs, including their points of entry and exit. This includes all domestic and foreign numbers and can also identify SIM swaps in a device. Foreign devices entering another national jurisdiction can be tracked to the same level of accuracy as domestic devices. Domestic devices going abroad can be tracked to the level enabled by the roaming network.

Proximity Alarms

Key locations, sensitive sites and vital installations can be digitally ring-fenced, or geofenced. When a number or handset of interest is already identified, they can be tracked in real-time to monitor their position relative to an exclusion area, and when they reach to within a certain proximity of that exclusion area an alarm is set off, triggering an alert that certain handsets or numbers have entered an exclusion zone. This type of sensitive site geofencing can also be used to identify if any mobile subscribers in an area have been in proximity with a known suspect at any time in the past. This information could help establish that the target is with one or a number of yet-unknown associates – who, with this intelligence, would become potential persons of interest, suspects or even threats.

Historic Tracking and Live Tracing

MNOs can replay targets' movements through time by exploiting CDRs, which all MNOs store. Increasingly, however, MNOs are also storing a much more detailed form of location data history: through logging of all passive signalling and paging interactions with the network, as well as logging timing advance data. While timing advance data offers a range within which a handset was connected to a particular cell (azimuth), the logging of passive signalling and paging exchanges with the

network creates an incredibly-rich location data record of the subject. Since this data is generated *passively*, meaning without active use of the network, and only requires that the handset be switched on and connected to a network, MNOs that log signalling data have effectively turned their customers into unknowing ankle-tag wearers. In the context of a live trace, all of these technologies (and more) are available to state security agencies, in addition to assisted-GPS geolocation and triangulation through continuous 'pinging' of the handset.

4. The Intersection of Militarised Tech and State Crime in Kenya

This case study looks at how state security services in Kenya derive ubiquitous technical intelligence from the near-monopoly MNO, Safaricom PLC for border monitoring, predictive identification of 'terror' suspects, tracking of suspects and dissidents – at times with software and algorithms supplied by the British company, Neural Technologies Ltd. In particular, the study focuses on a predictive analytic algorithm, 'Find My Friend', designed by Neural Tech. It then demonstrates how Kenyan security services utilise the data in a targeting cycle that very often ends up in the abuse or murder of targets, be they criminal suspects or dissidents. This is by no means an isolated, or historically anomalous practice for state forces in Kenya. That the Kenyan state employed a "systematic, widespread and well-planned strategy to execute individuals" was the conclusion reached by a United Nations investigation into the killing of more than a thousand gang members, insurgents, petty criminals and political protestors following the 2007 elections (Alston, 2009, p. 2). Little has changed since.

State Crime in Kenya

Kenya state criminality has endured since, through the so-called 'war on terror', with extraordinary rendition, enforced disappearance and summary execution of suspects and dissidents, including the employment of a CIA-run covert paramilitary squad (Shabibi, 2020a). In the almost-twenty years since the UN report cited above, the number of police killings and disappearances of terrorism or other criminal suspects has steadily increased, such that by 2017 Kenya accounted for two-thirds of police extrajudicial killing cases in Africa (Apollo, 2017). And since Kenya's crackdown against anti-finance bill protestors in spring/summer 2024, those figures have ballooned (Mureithi, 2024). It is in this climate of state criminality and impunity that the invasive – and likely both unconstitutional and unlawful – surveillance and targeting practices described below take place and should be understood. For scholars of Kenyan history, it is part of an enduring legacy of state crime

and impunity, whose modus operandi can be readily traced to Britain's brutal colonisation, exploitation and repression of insurgencies in Kenya; the best known among them being the 'Mau Mau' uprising (Shabibi, 2024a).

To conduct predictive analytics, bulk and targeted surveillance, relatively resource-starved Kenyan police turned to ubiquitous data collectors, to exploit their datasets. The previous sections of this research paper established Safaricom as a big tech company that plays a central role in Kenyan digital public infrastructure, and in enabling social life. Given Safaricom's near-monopoly status in Kenyan telecoms and mobile money payments, and that nearly every Kenyan carries Safaricom in their pocket, it follows that Safaricom is *the* ubiquitous sensor and data collector in the country. In other words, the Safaricom network is a key node in the Kenyan state's ubiquitous technical surveillance. It is in this context that a former Kenyan National Intelligence Service (NIS) officer explained to the author that state capture of Safaricom meant capture of the country. In return, Safaricom would enjoy preferential treatment for security and other state digital infrastructure contracts, the source alluded: "You need [Safaricom]. They are the best. They have the biggest field of data... [Safaricom] wouldn't have the monopoly if they didn't have the quid pro quo." (TSG, 2017)

Telecoms and Policing as an Integrated Operation

For years, Kenyan state exploitation of Safaricom's datasets took place through time-consuming liaison, as the author established through interviews with current and former Safaricom employees. Law enforcement requests for historic data and live tracing would be passed to Safaricom officers, who then channelled them through analysts to conduct the data extraction and geolocation of suspects. But given the police's eventual reliance on the Safaricom network to conduct surveillance, and the scale at which it grew, that process soon became unworkable. Such requests would take many hours, if not days, depending on urgency. In the eyes of both Kenya's Directorate of Criminal Investigation (DCI) and Safaricom, this arrangement was neither efficient nor fast enough.

A former Safaricom employee who had direct knowledge of liaison with DCI told the author that a plan was hatched to resolve these bottlenecks: at meetings between DCI and Safaricom and the latter's HQ the parties discussed "ways of improving and making it easier for [DCI] to get their requests". The solution? In 2012, Safaricom invited DCI officers to 'attach' to its headquarters, forming a Law Enforcement Liaison Office (LELO) composed of DCI and intelligence officers, overseen by a Safaricom employee. Access to Safaricom subscriber communications data by DCI officers became streamlined through two principal means: a) via DCI officers attached to Safaricom and sat within LELO, and b) via web-based remote access devices assigned to specialist tactical policing teams of DCI. In both

instances, the capabilities were designed by British company, Neural Technologies Ltd. The manager of that project, Jeff Cheatham, confirmed to the author that the initiative had been driven by Safaricom, which is part-owned by the Kenyan government:

> It was Safaricom that they thought they knew that the law enforcement agent had to wait a while and they wanted to do better. So I believe actually it would be kudos to them of wanting to be able to provide better service and easier service. (Cheatham, 2018)

In the case of DCI access via LELO, Cheatham's team designed a 'law enforcement agency' module, that sat among other modules within a suite collectively (and somewhat misleadingly) known as 'fraud management software'. The law enforcement agency (LEA) module is an access-controlled interface that allows individual DCI officers to query the Safaricom system for communications data, M-Pesa (mobile money) data and other data held within the system, based on requests received from DCI field offices, as well as court orders. Also designed by Neural Tech, the second channel through which DCI access sensitive communications data of Safaricom subscribers is via web-based remote access devices assigned to specialist tactical policing teams of DCI, as well as Kenya's NIS. Cheatham explained the idea's origins to the author, acknowledging that such a project "would never fly in UK or US", due to privacy concerns:

> [I]t's fascinating and actually I thought it was groundbreaking and very forward thinking and I wish we could do that here in the [United] States, but I know that with the privacy laws, it just would never go over…So [Safaricom's] concept was, hey, the fraud system has all the fraud, has all the call record details anyway, the fraud system, our fraud system stores, every time you make a call: 'who's it from? Who's it to? the A and the B number, [and] what cell towers were you by at the time?' And it doesn't actually hold the content of what was spoken, but how long it was where you were, every SMS text message, every time you used your data plan, the IP address that you're at and the IP address you hit. So every little data element is stored and goes through our system for analysis. And so since all that information is already there, [Safaricom] thought, hey, can we somehow hook it up to where the law enforcement or anybody else can remotely access this automatically? (Cheatham, 2018)

Cheatham's colleagues at Neural Technologies then set about designing browser-based remote access to the Safaricom system to satisfy the Kenyan police's desire for quick, unbridled access to subscriber data:

> [Y]ou could be from a law enforcement agent, the police officer, and they could enter in a simple request of like, 'Hey, here's the phone number, I found this phone at the scene at a crime. Here's the phone number. I want to know what numbers did it call or where was it used last or what SMS'. They have to be very specific still: 'I want the SMS text records, I want the data plan. What was going on? What webpages were being viewed? Who called them?' (...) So I'm an officer; I arrive at the scene at a crime quick on my mobile phone. I want to connect to Safaricom and get the call records immediately before the killer gets away too far because maybe he's still around here somewhere; which is an awesome idea, which, again I know would never fly in UK or US, but I love the concept and I was really impressed with their ideas. (Cheatham, 2018)

'Small Wars, Big Data'

Much of the Kenyan state's discourse on fighting crime and counterinsurgency is framed in terms of wars on 'terror', poaching, gangs and smuggling. In geographical terms, the three of these categories (war on terror, anti-poaching and counter-smuggling) are often related to the Kenya-Somalia border, with pre-emptive suspicion placed on ethnic Somali communities, as well as the predominantly Muslim coastal region. Similarly, anti-poaching initiatives are typically focused on areas where ethnic Borana or Somalis reside. Inevitably, therefore, systems of surveillance, pre-crime analysis and targeting disproportionately affect Muslims and ethnic Somalis, who make up the bulk of the border and migrant population in Kenya, since these systems automate existing attitudes, biases and criminal investigative priorities.

The investigation and targeting of criminal gangs and insurgents is often framed in the counterinsurgency (COIN) metaphor of 'finding needles in a haystack'. In other words, the so-called 'small wars' of COIN are an intelligence-led activity. As such, the entirety of the haystack needs to be sifted using data-driven techniques to identify 'digital footprints' resembling those of the targets and their accomplices (Berman, Felter and Shapiro, 2018). With the modern age, and the proliferation of sensors, offering what US officials describe as a 'tsunami' of data to sift through (Manson, 2026, p. 37), the fighting of so-called 'small wars' is now deemed primarily an exercise in big-data collection, exploitation and investigation. Naturally, it is presented by its advocates as a less harmful, less arbitrary COIN tactic in the state power repertoire, whose history is dominated by brutal, arbitrary violence.

To meet this challenge, a decade ago Neural Technologies explained that African MNOs were "under more pressure than ever to identify and report potential criminal activity". Neural Tech's deputy CEO at the time, Luke Taylor, announced that his company was "honoured" to be supporting Safaricom, "aiding the

crackdown on criminal activity such as poaching and terrorism" (*OSS News Review*, 2016). Part of this effort is the pre-crime modelling of each subscriber, wherein one Neural solution is to model each Safaricom user and their 'organisational behaviour', meaning their actions and interrelations with one another, "to detect scenarios that are indicative of criminal activity such as smuggling, poaching and terrorism" (*OSS News Review*, 2017). In a separate interview, Taylor was more candid about the outcome, saying that he was considering solutions to help Kenyan police who were "looking to use the telco [Safaricom] information" to map criminal networks "and close them down." He then explained how Kenyan police would utilise data made available through its software:

> We've been looking at situations where law enforcement have already identified an individual – caught him with an elephant tusk under his arm – they're looking at his phone, looking to track all the people he's been traveling with and communicating with... Law enforcement is looking to use the telco information to find the gang, and close them down. (Priezkalns, 2016)

Safaricom and Neural Technologies' partnership worked so well that two years later, the British company was preparing to go much further to facilitate Kenyan law enforcement's access to Safaricom data. But by this point Neural had become publicly circumspect about its role in surveillance and targeting, so the author visited Neural Technologies' office to meet its staff. "We call it 'Find my Friends'", joked Adrian Harris, former director of new products at Neural Technologies in an interview. 'Find My Friends' was a prototype visualisation function that allowed law enforcement officers to predictively profile Kenyans and flag them for further investigation based on their patterns of movement and association.

As explained by Harris, it works like this: a Kenyan officer wants to investigate a particular individual. They look up the person's phone number and using the tool's map search function, they map the target's movements by triangulating the mobile masts to which their phone connects as they move across Kenya. This form of tracking does not require phone use (call data events) but the phone to simply be on, due to passive location updates and signalling messages occurring at regular intervals. The algorithmic tool also analyses Safaricom's dataset to identify other individuals who may be moving in the same way as the target, to whom they might be associated, proactively identifying new 'suspects' by mapping how they use their phones. On this point, Harris added, defensively: "We're not actively looking for you," he explained. "All we're doing is we're looking at that information that we've been capturing and continue to capture as you go along" (Harris, 2018).

Kenyan constitutional human rights lawyer, Haron Ndubi reviewed the author's findings and commented: "You cannot treat all of us as suspects", he said. "To have some random mechanism where you want to check on everyone and see who they're

talking to…it's already criminal in itself" (Ndubi, 2024). Neural Technologies did not respond to repeated requests for comment, including that it clarify what due diligence it conducts on end users of its technologies. Safaricom has also not provided substantive comment on the author's investigation, a summary of which was originally published in October 2024 (Shabibi and Lauterbach, 2024). Instead, in a terse email response, the MNO denied breaching its customers' right to privacy even after being presented with evidence of the contraventions:

> Safaricom has always taken our responsibility to protect customer data very seriously. We prioritise the privacy of our customers and are dedicated to upholding our customers' trust through protecting their privacy," said a Safaricom spokesperson in a statement.
>
> We safeguard all data in line with our obligations and the law, and we only release call data records to verified law enforcement authorities while required via a court order. While we cannot discuss individual cases, we have always been transparent and honest in how we engage with our stakeholders, and we will continue doing so in order to maintain the trust that we have built over the years. (Karanja, 2024)

Big Tech, Big Data and State-Corporate Crime

Separate journalistic investigations by the author established the mechanics of the so-called 'kill chain' in CIA-backed covert Kenyan paramilitary police squad. Though only one element in a constellation of police, intelligence, paramilitary and special force activity in domestic repression and broader state violence, that police squad is one of the most important; it was created by the CIA, in partnership with its Kenyan counterparts, to 'neutralise' high-risk and/or 'high-value' targets – typically people suspected of links to 'terrorism' (Shabibi, 2020b). Invariably the intelligence, paramilitary and police officers interviewed spoke at length about the key surveillance elements that underpin the targeting cycle, which prioritises kill over capture (Shabibi, 2024b). Such outcomes suited decision-makers back at CIA headquarters and the White House, according to a former senior US official based in Africa. "There's one stat that counts more than convictions. And that's neutralisation of a criminal organisation" (Shabibi, 2020a).

Multiple current and former commandos of the CIA-backed squad told the author that partner (liaison) intelligence officers would systematically exploit the Safaricom network for both intelligence gathering and tactical policing operations. For intelligence gathering on a suspect, Kenya's services turn to the most ubiquitous sensor, a key element of digital public infrastructure, that almost everyone carries in their pocket: a Safaricom line. When a suspect is not already identified

through pre-crime analytics, but through more conventional investigative means (e.g. a human source tip off), Kenyan intelligence officers use stored call data records and administrative signalling logs to identify the suspect's pattern of life, and their social, business or other networks. When the target handset is on, a serving officer of the CIA-backed paramilitary squad explained, the suspect would be live traced through triangulation of signals against Safaricom cell towers. "[T]here's always Safaricom, where you can track somebody", he explained, adding:

> It will tell you he's within a radius…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 10m from the guy. So that is the time now the guys can disembark… and manually cordon the area. (SIC, 2017)

In short, the Safaricom network offers the rough location of the target. As recalled above, depending on type of phone (dumb vs GPS-enabled smartphone), and the number of masts within range, the estimated location of the target can vary. From there Kenyan intelligence officers accompanying the commandos deploy with what they colloquially refer to as a 'sensor', otherwise known as an 'IMSI catcher'.[9] An IMSI catcher is designed to simulate and mimic a cell tower, while offering the strongest available signal, prompting all phones within its vicinity to switch to it. The IMSI catcher is then able to establish the target's precise location, including elevation, and enables interception of traffic while still functioning as a cellular network, so as not to betray the covert operation.

So-called 'targets' of police and paramilitary police operations, particularly among the marginalised communities of Kenya, frequently end up dead: gunned down on the spot, police typically plant weapons and then claim that a 'shootout' occurred, forcing the officers to use lethal force (Lauterbach and Shabibi, 2021). "Kenyan police are a law unto themselves. They kill often, with impunity," the United Nations investigation into the killing of more than a thousand gang members, insurgents, petty criminals and political protestors following the 2007 elections declared (Alston, 2009, p. 2). Its addendum elaborates: "Most troubling is the existence of police death squads operating on the orders of senior police officials…". This cycle of impunity is reinforced by the employment of clandestine and covert operating tactics used by tactical paramilitary and other policing units of the Kenyan state, buttressed by rituals of cover up and denial by the Kenyan state institutions (Shabibi, *forthcoming* 2026).

When a suspect is captured and prosecuted, cell site data (and specifically CDRs) is often a key dataset used to prosecute. Furthermore, where the suspect's handset

[9] Otherwise known as an 'IMSI grabber', or more commonly as 'StingRay', which is a Harris Corporation manufactured version.

is seized, universal forensic extraction devices are used to unlock and recover all data, far beyond what a user assumes to be stored on their device (Lauterbach and Shabibi, 2021). As noted earlier, an investigations and prosecutions manual written by the British Foreign Office for Kenya's Anti-Terrorism Police Unit (ATPU), lists call and SMS data as "critical evidence" to seek in 13 of 37 categories of offences under terrorism, organised crime and firearms legislation. The same data that is so useful to the state in targeting, tactical operations *and* prosecution is also just as useful to victims of state crime. In particular, when state officers or agents forcibly disappear a target, the movements of their phone, powering on and off, and decoupling of the SIM card and handset to be used separately, can all be tracked. And this data *can* be obtained from MNOs – when they were willing to share it. This makes Big Tech MNOs like Safaricom gatekeepers to the secrets of state-enforced disappearances.

When Kenyan police face accusations of murder or enforced disappearance, Safaricom's actions can impede the pursuit of justice. One way the MNO has done this is by claiming that CDRs older than 90 days are automatically deleted, implying that information is no longer held, which misleads lawyers and the courts. When compelled – by court order – to release the data it admits to having, the company also systematically routes requests for CDR evidence to police officers embedded in its headquarters, posing a conflict of interest when police are themselves implicated in the allegations. Unsurprisingly, the CDR data released by Safaricom in cases of suspected state crime bears signs of tampering; missing crucial data, such as location data for suspects' and victims' phones around the time of the crimes. Forensic experts consulted over the records agreed with the author's analysis – and, as such, the records reluctantly disclosed by Safaricom can obfuscate crimes involving the Kenyan state, as well as the victims' whereabouts. In the International Criminal Court's case against Kenyan officials, including former President Uhuru Kenyatta, the former lawyer representing victims told the author that the allegedly-fabricated records disclosed by Safaricom played a "considerable role" in the case's collapse (Gaynor, 2019).

By contrast, when it comes to aiding the Kenyan state, Safaricom gladly turns over data on its subscribers. CDRs provided by Safaricom have played a key role in the police pursuit of well-known cases, such as "pinning" the conviction of the 2010 Kampala bombing suspects. Richard Frankel, the US FBI's Special Agent In-Charge of the investigation into the attack on Westgate mall in Nairobi in 2013 explained that his team found SIM cards of the suspected attackers, which they gave to Safaricom. "That's really what led us to some of the targets, identifying where some of them were and who they were talking to", Frankel told the author, adding "Safaricom supported us in every manner that they could" (Frankel, 2018). But Safaricom's readiness to support law enforcement is far from anecdotal. Multiple

court cases have found the telecoms company providing unlawful and unconstitutional access to its data for police (Munguti, 2025; Wasuna, 2021). Against this backdrop, public interest lawyers have expressed exasperation at what they perceived to be Safaricom's systematic frustration of justice, and a sense of powerlessness in the face of state and corporate impunity. Victor Kamau, former Deputy Director of the Kenya National Commission on Human Rights told the author, "By its reluctance to cooperate with our investigations… [Safaricom] is complicit with their disappearances" (Kamau, 2018).

5. Conclusion

The overrepresentation of commercial spyware in state surveillance investigation and accountability initiatives has helped to obscure the most common vector for mobile surveillance; telecoms network themselves. For human rights NGOs and other civil society advocates, this has meant that advancements in telecoms infrastructure, which have enabled exponentially more accurate location intelligence, have been largely overlooked. Meanwhile, the past decade's quiet yet systematic transference of military intelligence analytic methods, buttressed by machine-learning algorithms, to everyday surveillance of telecoms in the Global Majority is arguably the greatest threat to civic freedoms. By embracing the intelligence community concept of UTS, and its thinking around surveillance practice, the human rights community will be better equipped to address the modus operandi and vectors of state surveillance practice in the Global Majority. Undoubtedly, telecoms networks are a key node in UTS, not only because of their ubiquitous use, their centrality in digital public infrastructure and social life, but also because of the sheer amount of data that is automatically logged, enabling historic and live geolocation of targets, as well as link analysis of their networks, and pattern of life.

As we have seen through the Kenya case study, the exploitation of telecoms networks as part of UTS in states that are routinely criminal yet unaccountable, presents a grave and pervasive threat to all phone users. This is particularly the case in Kenya, where access to the Safaricom network is essential for access to public infrastructure, including banking and other financial services. As always, it is the most marginalised communities – such as the ethnic Somali and Muslim border and coastal communities of Kenya – that bear the brunt of pre-emptive suspicion that pre-crime analytics of telecoms networks entail. After all, to fight 'small wars', one needs to sift through 'big data' – or so the current counter-insurgency logic goes. The fusion of Big Tech telecoms company, Safaricom and Kenya's Directorate of Criminal Investigation, into an integrated operation, where police officers are attached to Safaricom HQ to enjoy direct access for historic and live investigations

may be a striking example. But it is broadly reflective of the cosy relationship that Big Tech is well known to enjoy with the state.

With every Safaricom user assigned risk scoring to assess the likelihood of their role in grave crimes of terrorism and poaching, and with telecoms operators logging 'digital footprints' for years, telecoms data is vast trove for police investigators – and a go-to dataset, particularly in resource-starved states. As with police the world over, Kenyan law enforcement routinely use said data to investigate and prosecute crime – and to locate missing persons. Such data could easily be exploited in the same way, in the public interest. Indeed, savvy advocates in a handful of countries where the rule of law is stronger have exploited telecoms data to great effect. However, in Global Majority states like Kenya, where literacy around the value of telecoms (cell site) data, and how to exploit it, is low, opportunities to effectively investigate state crime are routinely missed. In particular, the utility of cell site investigations to the tracing of missing persons, or in Kenya's case the longstanding practice of state-enforced disappearance, cannot be overstated. But in a country where the police and near-monopoly telecoms company are an integrated operation to the mutual benefit of one another, Safaricom routinely throws obstacles before advocates seeking to investigate state crime. Sat atop of the nation's most important and ubiquitous surveillance dataset, with years of digital footprints for most of the population, it renders the telecoms company the gatekeeper to the secrets of Kenya's disappearances. And the same applies to mobile operators the world over.

As bleak as the landscape painted above is, a positive note is necessary. NGOs and other human rights organisations can pivot towards a better understanding of the risks posed by telecom network surveillance, and in-turn they can offer activists, dissidents and protestors effective countermeasures, beyond extreme spyware-specific measures such as Apple's 'lockdown mode'. The second optimistic note to make here is that with sufficient will, resources, and civil society donor support, advocates can effectively use the courts to obtain, exploit and visualise telecoms (cell site) data to investigate and solve state crime, particularly enforced disappearance. And when the telecoms company proves recalcitrant, and more intent on protecting the state than the nation, boycotts are possible. This is of course far easier said than done: in Kenya, as with many Global Majority companies, Safaricom provides a wealth of DPI and other financial services, and its mobile money transfer service is a lifeline for many. Choosing to opt-out is far from easy as peaceful protest in Kenya is often being met with brutal state repression and violence. So, it is worth recognising that – when done en masse – a Kenyan's decision to port their number over from Safaricom to a rival telecoms company, may be one of the simplest yet profound acts that can be done in the service of the nation.

6. Bibliography

About Lockdown Mode (2026). Apple Inc. Available at: *https*://support.apple.com/en-gb/105120 (Accessed: 7 August 2026).

Adekunte, P.A., Sadiku, M.N.O. and Sadiku, J.O. (2024) 'Ubiquitous Technical Surveillance: An Introduction', *International Journal of Trend in Scientific Research and Development*, 8(4). Available at: https://www.ijtsrd.com/papers/ijtsrd67144.*pdf*.

Alston, P. (2009) *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston: addendum*. A/HRC/11/2/Add.6. United Nations. Available at: https://digitallibrary.un.org/record/*657905* (Accessed: 29 May 2024).

Apollo, S. (2017) 'Kenya Tops Africa in Police Killings', *Daily Nation*, 23 February. Available at: https://web.archive.org/*web*/20170223233952/https://www.nation.co.ke/news/Kenya-top-Africa-police-shootings/1056-3824890-1183k27/ (Accessed: 24 April 2024).

Bell, M. (2025) *Data Security Concerns Rise as Surveillance Becomes Ubiquitous*. U.S. Army. Available at: https://www.army.mil/article/287760/data_security_concerns_rise_as_surveillance_becomes_ubiquitous (Accessed: 7 August 2026).

Benner, K., Sanger, D.E. and Barnes, J.E. (2021) 'Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa', *The New York Times*, 3 December. Available at: https://www.nytimes.com/2021/12/03/us/politics/phone-hack-nso-group-israel-uganda.html?eafs_enabled=false (Accessed: 14 August 2026).

Bergman, R. and Mazetti, M. (2022) 'The Battle for the World's Most Powerful Cyberweapon', *The New York Times*, 28 January. Available at: https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html (Accessed: 14 August 2026).

Berman, E., Felter, J.H. and Shapiro, J.N. (2018) *Small Wars, Big Data: The Information Revolution in Modern Conflict*. Princeton University Press.

Betournay, S. (2026) 'CDR Analysis 101: What Call Detail Records Reveal in Investigations', *Penlink*, 14 May. Available at: https://www.penlink.com/blog/cdr-analysis-101/ (Accessed: 29 August 2026).

*Blurring the Line: How Militarisation of Tech is Reshaping Our Town Square*s (2025). Privacy International. Available at: http://privacyinternational.org/long-read/5669/blurring-line-how-militarisation-tech-reshaping-our-town-squares (Accessed: 10 January 2026).

Burns, W. (2022) 'The Role of Intelligence at a Transformational Moment', 14 April. Available at: https://www.cia.gov/static/Director-Burns-Speech-and-QA-Georgia-Tech.pdf.

Cheatham, J. (2018) 'Author's interview with Jeff Cheatham, former Neural Technologies project manager in Kenya'.

Costa-Roberts, D. (2015) 'AT&T Cooperated Extensively with NSA, Snowden Documents Reveal', *PBS News*, 15 August. Available at: https://www.pbs.org/newshour/politics/report-att-cooperated-extensively-nsa-sharing-billions-phone-email-records (Accessed: 8 January 2026).

Currier, C., Greenwald, G. and Fishman, A. (2015) 'U.S. Government Designated Prominent Al Jazeera Journalist as "Member of Al Qaeda"', *The Intercept*, 8 May. Available at: https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/ (Accessed: 8 January 2026).

Dwivedi, S. *et al.* (2020) '5G Positioning: What You Need to Know', *ericsson.com*, 18 December. Available at: https://www.ericsson.com/en/blog/2020/12/5g-positioning--what-you-need-to-know (Accessed: 7 August 2026).

Espiner, T. (2009) 'Vodafone Exec Warns Against Tech Regulation', *ZDNET*, 11 February. Available at: https://www.zdnet.com/article/vodafone-exec-warns-against-tech-regulation/ (Accessed: 8 January 2026).

Flynn, Michael T., Juergens, R. and Cantrell, Thomas L. (2008) 'Employing ISR: SOF Best Practices', *Joint Force Quarterly*, (50), pp. 56–61.

Frankel, R. (2018) 'Author's interview with Richard Frankel, former FBI Special Agent in Charge of the team that investigated the attack on the Westgate Mall in Nairobi, Kenya'.

'Freedom of Information request reference 02164629' (2026). Ofcom. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/about-ofcom/foi/2026/march/numbers-of-4g-and-5G-masts-in-the-united-kingdom.pdf?v=414904.

Gaynor, F. (2019) 'Author's interview with Fergal Gaynor, former lead counsel for victims at the International Criminal Court'.

Goodfriend, S. *et al.* (2026) 'Anatomy of an AI Kill Chain', *Airwars*, 28 July. Available at: https://ai-kill-chain.airwars.org/.

Grothoff, C. and Porup, J.M. (2016) *The NSA's SKYNET Program May Be Killing Thousands of Innocent People*, *Ars Technica*. Available at: https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/ (Accessed: 8 January 2026).

Harris, A. (2018) 'Author's interview with Adrian Harris, Neural Technologies CTO'.

Heath, B. (2015) 'U.S. Secretly Tracked Billions of Calls for Decades', *USA Today*, 8 April. Available at: https://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/ (Accessed: 29 August 2026).

Hern, A. (2018) 'Fitness Tracking App Strava Gives Away Location of Secret US Army Bases', *The Guardian*, 28 January. Available at: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (Accessed: 7 August 2026).

Holmes, R. (2026) 'Hundreds of UK Soldiers Exposed at Military Bases... by Their Strava Workouts', *The i Paper*, 3 April. Available at: https://inews.co.uk/news/hundreds-uk-soldiers-exposed-military-bases-strava-workouts-4314089 (Accessed: 7 August 2026).

Kamau, V. (2018) 'Author's interview with Victor Kamau, Deputy Director of the Kenya National Commission on Human Rights'.

Karanja, C. (2024) 'Follow Up: Safaricom: Opportunity to Comment on Forthcoming Publication'.

Kraska, P.B. (2007) 'Militarization and Policing—Its Relevance to 21st Century Police', *Policing: A Journal of Policy and Practice*, 1(4), pp. 501–513. Available at: https://doi.org/10.1093/police/pam065.

Lauterbach, C. (2015) *For God and My President: State Surveillance in Uganda*. Privacy International. Available at: https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf (Accessed: 15 August 2026).

Lauterbach, C. and Shabibi, N. (2021) '"Tacit Approval" for Killings: UK Foreign Office and Police Support to Kenyan Anti-Terror Unit "Operating Like a Criminal Gang" Revealed', *Declassified UK*, 11 February. Available at: https://www.declassifieduk.org/tacit-approval-for-killings-uk-foreign-office-and-police-support-to-kenyan-anti-terror-unit-operating-like-a-criminal-gang-revealed/ (Accessed: 30 May 2024).

Li, P., Fan, J. and Wu, J. (2025) 'Exploring the Key Technologies and Applications of 6G Wireless Communication Network', *iScience*, 28(5), p. 112281. Available at: https://doi.org/10.1016/j.isci.2025.112281.

MacAskill, E. *et al.* (2013) 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications', *The Guardian*, 21 June. Available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (Accessed: 8 January 2026).

Manson, K. (2026) *Project Maven: A Marine Colonel, His Team, and the Dawn of AI Warfare / Katrina Manson*. New York: W.W. Norton and Company.

Munguti, R. (2025) 'Safaricom Gave Student's Data to Police Without Court Orders, Over Post About President Ruto', *Daily Nation*, 9 September. Available at: https://nation.africa/kenya/news/safaricom-gave-student-s-data-to-police-without-court-orders-over-post-about-president-ruto--5186004 (Accessed: 15 August 2026).

Mureithi, C. (2024) '"Enforced Disappearances" Send a Chill Through Kenya's Protests', *The Guardian*, 15 August. Available at: https://www.theguardian.com/world/article/2024/aug/15/kenya-protests-disappearances (Accessed: 16 September 2024).

Muyanga, P. (2021) 'Court Declines to Bar M-Pesa Payments for Likoni Ferry Crossing', *Daily Nation*, 5 October. Available at: https://nation.africa/kenya/counties/mombasa/court-declines-bar-m-pesa-payments-for-likoni-ferry-crossing-3572932 (Accessed: 15 August 2026).

Ndubi, H. (2024) 'Author's interview with Haron Ndubi, Kenyan constitutional lawyer'.

New U.S.-led Actions Expand Global Commitments to Counter Commercial Spyware (2024). United States Department of State. Available at: https://2021-2025.state.gov/new-u-s-led-actions-expand-global-commitments-to-counter-commercial-spyware/ (Accessed: 7 August 2026).

OSS News Review (2016) 'Neural Technologies and Safaricom Win Global Telecoms Innovation Award', 31 May. Available at: https://www.ossnewsreview.com/neural-technologies-safaricom-win-global-telecoms-innovation-award-4956 (Accessed: 7 August 2026).

OSS News Review (2017) 'Neural Technologies Shortlisted for 2017 GSMA Glomo Awards', 4 February. Available at: https://www.ossnewsreview.com/neural-technologies-shortlisted-2017-gsma-glomo-awards-5084 (Accessed: 7 August 2026).

Priezkalns, E. (2016) 'Demanding Change, with Neural Technologies', *CommsRisk*, 14 November. Available at: https://commsrisk.com/demanding-change-with-neural-technologies/ (Accessed: 7 August 2026).

'Protecting U.S. National Security and U.S. Personnel from Ubiquitous Technical Surveillance and Commercial Data Exploitation' (2025). Available at: https://www.armed-services.senate.gov/imo/media/doc/sherman_opening_statement.pdf.

Safaricom - Our Commitment. Available at: https://www.safaricom.co.ke/about/who-we-are/our-story (Accessed: 6 March 2026).

Sanchez, S. (2020) *Ubiquitous Technical Surveillance: Counterintelligence Bliss, or Nightmare?* Available at: https://doi.org/10.13140/RG.2.2.23516.16002.

Sankritik, A. and Shetty, S. (2025) *Digital Public Infrastructure: Setting Standards with the Hourglass Model*. Working Paper. World Bank Group. Available at: https://thedocs.worldbank.org/en/doc/5fdfbc4891d5c9f0942f7e0f86a72e05-0050062025/original/Abhishek-Sankritik-Digital-public-infrastructure.pdf (Accessed: 6 March 2026).

Shabibi, N. (2020a) 'Revealed: The CIA and MI6's Secret War in Kenya', *Declassified UK*, 28 August. Available at: https://declassifieduk.org/revealed-the-cia-and-mi6s-secret-war-in-kenya/.

Shabibi, N. (2020b) 'The Militarisation of US/Africa Policy: How the CIA Came to Lead Deadly Counter-Terrorism Operations in Kenya', *Declassified UK*, 28 August. Available at: https://declassifieduk.org/the-militarisation-of-us-africa-policy-how-the-cia-came-to-lead-deadly-counter-terrorism-operations-in-kenya/.

Shabibi, N. (2024a) 'Night Terror', *Material Crimes* (Season 2). Available at: https://materialcrimes.com/Night-Terror.

Shabibi, N. (2024b) 'Victims of CIA Kenyan Hit Squad Win Compensation After Our Exposé', *Declassified UK*, 18 April. Available at: https://www.declassifieduk.org/victims-of-cia-kenyan-hit-squad-win-compensation-after-our-expose/ (Accessed: 29 May 2024).

Shabibi, N. (2025) 'Explainer: Your Phone and Surveillance: Five Things You Should Know', *Daily Nation*, 18 June. Available at: https://nation.africa/kenya/blogs-opinion/blogs/explainer-your-phone-and-surveillance-five-things-you-should-know-5081236 (Accessed: 6 August 2025).

Shabibi, N. (*forthcoming* 2026) 'Clandestine Manoeuvres and Rituals of Denial: The CIA's Covert Counter-Insurgency in Kenya', in T. MacManus *et al*., *Routledge Handbook of State Crime*. Routledge.

Shabibi, N. and Lauterbach, C. (2024) 'Exclusive: How Kenyan Police Use Mobile Phones to Track, Capture Suspects', *Daily Nation*, 29 October. Available at: https://nation.africa/kenya/news/exclusive-

how-kenyan-police-use-mobile-phones-to-track-capture-suspects-4804416 (Accessed: 7 December 2024).

Sherman, J. (2025) 'Ubiquitous Technical Surveillance Demands Broader Data Protections', *Lawfare*, 25 July. Available at: https://www.lawfaremedia.org/article/ubiquitous-technical-surveillance-demands-broader-data-protections (Accessed: 7 August 2026).

SIC (2017) 'Author's interview with a current officer of the Recce Special Anti-Terror Team, who previously worked with the RRT on operations'.

Spyware Accountability Initiative, With Seed Funding From Apple and Leading Philanthropies, Announces Over $4 Million in Grants to Address the Harms of Spyware on Civil Society (2024). Ford Foundation. Available at: https://www.fordfoundation.org/news-and-stories/news-and-press/news/spyware-accountability-initiative-with-seed-funding-from-apple-and-leading-philanthropies-announces-over-4-million-in-grants-to-address-the-harms-of-spyware-on-civil-society/ (Accessed: 7 August 2026).

Spyware and State Abuse: The Case for an EU-Wide Ban (2025) *European Digital Rights (EDRi)*. European Digital Rights. Available at: https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/ (Accessed: 7 August 2026).

Telco Hall of Shame: Vodafone (2013) 'Telco Hall of Shame: Vodafone', 29 January. Available at: https://www.accessnow.org/hall-of-shame-vodafone/ (Accessed: 28 August 2026).

Thomas, D. (2026) 'Top Companies in East Africa 2026: Tanzania's Growing Influence', *African Business*, 12 May. Available at: https://african.business//2026/05/trade-investment/top-companies-in-east-africa-2026-tanzanias-growing-influence (Accessed: 28 August 2026).

TSG (2017) 'Author's interview with a former Kenyan National Intelligence Service officer'.

Wasuna, B. (2021) 'Snooping, Digging, Tracing Calls: How Detectives Bend the Rules to Spy on You', *Daily Nation*, 5 April. Available at: https://nation.africa/kenya/news/snooping-digging-tracing-calls-how-detectives-bend-the-rules-to-spy-on-you-3349164 (Accessed: 15 August 2026).

Wessler, N.F. (2019) 'The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In', *American Civil Liberties Union*, 28 June. Available at: https://www.aclu.org/news/privacy-technology/supreme-courts-most-consequential-ruling-privacy-digital (Accessed: 9 January 2026).

Wilkinson, R., Krasodomski, A. and Wilkinson, I. (2025) *The Case for Expanding Digital Public Infrastructure: How Open, Scalable Technology Can Serve Citizens, Preserve Sovereignty and Save Money*. London: Royal Institute of International Affairs. Available at: https://chathamhouse.soutron.net/Portal/Public/en-GB/RecordView/Index/207695 (Accessed: 6 March 2026).

'Wireless Call Location Services: Tech Note' (2007). U.S. Department of Homeland Security. Available at: https://www.dhs.gov/sites/default/files/publications/WirelessCallLocation_TN_1107-508.pdf.

Wolfgang, B. (2026) 'The Danger of Digital Footprints: How "Ubiquitous Technical Surveillance" Threatens U.S. Military', *The Washington Times*, 27 May. Available at: https://www.washingtontimes.com/news/2026/may/27/danger-digital-footprints-ubiquitous-technical-surveillance-threatens/?srsltid=AfmBOopAN4GxspxKGKqlz5vo4wPchXhWTccd9SR7v6fqVvWWHJEN_tp0 (Accessed: 7 August 2026).

Yardley, M. *et al.* (2018) *Lowering Barriers to 5G Deployment*. Analysis Mason. Available at: https://www.connectivityuk.org/wp-content/uploads/2018/07/BSG-Report-Lowering-barriers-to-5G-deployment.pdf.