African Journal on Privacy & Data Protection

To cite: CA Khamala 'Digital surveillance and big data: Balancing the rights to privacy and security in Kenya' (2024) 1
African Journal on Privacy & Data Protection 176-206

Digital surveillance and big data: Balancing the rights to privacy and security in Kenya

*Charles A Khamala**
Senior Lecturer, Africa Nazarene University Law School; Academic Leader, Criminal Justice and Security Management

Abstract:

Education, personal identity and democracy flourish in private. Generalised surveillance of disenchanted groups stifles them. Although the African Charter on Human and Peoples' Rights is silent on the right to privacy, Kenya's Constitution expressly protects against surveillance abuse. Informed consent is required from data subjects prior to collecting or sharing their personal information. Yet, Kenyan courts have upheld laws and policies introducing generalised surveillance. The conundrum confronting Kenya's judiciary regarding surveillance of mobile telephone data is: If counter-terrorism relies on mass surveillance, such policies necessarily violate privacy rights, in the guise of enhancing security. Nonetheless, enhancing the state's surveillance capacity to intercept digital communications was accepted by the Court as a justifiable violation of privacy rights. Conversely, in *Communication Authority of Kenya v Okiya Omtatah Okoiti*, the Court of Appeal observed that globally, the theft of mobile phones and proliferating counterfeit devices have become major regulatory concerns. Problematically, it

* PhD in Droit Privé (Sciences Criminelles) Université de Pau et des Pays de l'Adour (France); LLM (London) LLB (Nairobi); PGDip KSL; [email] chalekha@yahoo.co.uk; ckhamala@anu.ac.ke.

reversed the High Court's prohibition on generalised surveillance. Subsequently, in *Katiba Institute v Attorney General*, the High Court directed the state to conduct a data protection impact assessment as the Data Protection Act requires. In April 2023, the Supreme Court dismissed the Law Society of Kenya's appeal seeking to stop the CAK embarking on a device management system, which threatens to surveil subscribers. Three conclusions emerge. First, Kenya's DPA accords absolute governmental power to gather personal data unrelated to national security or suspicion of crime. Second, the Court of Appeal's *Mobile Telephones* determination is oblivious to the chilling effect that any generalised surveillance creates even on groups that value confidentiality. Third, neither the National Intelligence Services Act nor the Prevention of Terrorism Act protect citizens' communications from limited interception. It is preferable to introduce similar provisions authorising interception of specific communications in other legislations to facilitate investigation of serious organised crimes.

Key words: chilling effect; data protection; group privacy; human dignity; informed consent; intercept communications; secret intelligence

1 Introduction

Traditional English common law knew no right to privacy. This was held in *Wainwright v Home Office*[1] where, despite being strip-searched with excessive force by prison officers, a visiting mother and son had no cause of action for a privacy violation. Privacy rights were first recognised in the late twentieth century law of torts. Nonetheless, individuals who make such claims must not only identify their tortfeasor. They must also specify the remedies sought. Yet, simply hacking someone's correspondence without disclosing its information to a third party makes the concrete harm difficult to substantiate. This is because the law does not concern itself with trivialities.[2] Worse still, big data's harmful potential may remain unknown at the point of gathering. Significantly, digital data is collected over long durations from numerous nondescript persons, without a pre-established purpose.[3] Only upon subsequent analysis by computer algorithms does it produce statistical correlations with informative value. The results invariably reveal behaviour patterns of individuals or groups in websites frequented by internet users or cryptic codes contained in emails or other electronic messages. Emergent information may give governmental authorities reason to suspect an individual of engaging in terrorist activities or violating other laws. Although liberal democratic constitutions empower governments to produce public goods, state power is limited by individual rights. Yet, because

1 [2003] QB 195, 205-6; [2004] 2 AC 406.
2 B van der Sloot 'Is the human rights framework still fit for the big data era? A discussion of the ECtHR's case law on privacy violations arising from surveillance activities' in S Gutwirth, R Leenes & P de Hert (eds) *Data protection on the move current developments in ICT and privacy/data protection* (2016) 415.
3 Van der Sloot (n 2) 413.

warrantless mass surveillance technology is inherently invasive, it violates the personal sphere. Therefore, to safeguard privacy rights, data protection legislation has proliferated worldwide. These laws purport to protect data controllers, comprising persons who gather and control information, against privacy breach lawsuits. In pertinent part, section 30(1) of Kenya's Data Protection Act (DPA) precludes data controllers or processors from processing personal data, unless such processing is necessary to protect the data subject or other individual's vital interests; or to perform a public interest task or in the exercise of the controller's vested official authority; or to perform any task by a public authority.[4] To the extent that this provision permits mass surveillance, it may therefore overreach section 3's intended purpose of protecting the privacy of individuals as read with section 25's data protection principles. This anomaly is attributable to big data's abstract nature. Consequently, individuals may be unaware of their personal data's excavation and disclosure to third parties, whether by fellow citizens using smart phones, or by companies' tracking cookies or even by the government using covert surveillance.[5]

The essential problem with all surveillance is that while potential harms are comparatively manifest, its benefits are inconspicuous. Many terrorist operations that covert intelligence helps foil, remain unknown to citizens. Moreover, the act of looking for terrorists, as Donoghue observes, 'may well involve obtaining information about a large number of people'.[6] Thus, surveillance operations delve deep into the state's social and political life.[7] Van der Sloot concludes that difficulties arising from mass surveillance operations and big data analytics by states cannot be characterised as human rights violations, but instead should be understood as demands for enhanced governance and a fair hearing, underpinned by legality and legitimacy principles.[8] The purpose of this article, therefore, is to construct a normative framework to examine big data's impact on privacy rights. The objective is to evaluate the constraints of mass surveillance through big data in the Kenyan context. This issue confronts Kenya's judiciary with numerous challenges by citizens against executive overreach regarding surveillance by big data. For example, in 2020 at the Supreme Court, the Law Society of Kenya challenged the Communications Authority of Kenya's installation on mobile networks of the device management system (DMS). The DMS sought to enable authorities to hear phone conversations and see mobile money transaction messages.[9]

4 Sec 30 Data Protection Act 24 of 2019 (DPA).
5 Van der Sloot (n 2) 414.
6 LK Donoghue *The cost of counterterrorism*: *Power, politics, and liberty* (2008) 186.
7 S Chesterman *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty* (2011).
8 Van der Sloot (n 2) 434.
9 K Abuya 'Law Society of Kenya seeks to stop installation of spying tool by state' *techweez* 10 June 2020, https://techweez.com/2020/06/10/lsk-ca-kenya-dms-case/ (accessed 31 January 2023).

The next part of the article compares different approaches to privacy. Among liberal varieties, narrow approaches focus either on intimacy, privacy, embracing intimate information, access or decisions. Broad approaches include rights not to be pushed. They emphasise the right to be 'let alone' and relations between individuals. Privacy rights, therefore, should protect secrecy, anonymity and solitude.[10] Both these approaches protect liberty from external interference. They correspond to rule utilitarianism and act utilitarianism, respectively. Ultimately, protecting honour militates against stripping dignity away from a meaningful private life. Therefore, psychologists indicate that cultivating dignity demands more than just a secluded private place. Part 3 of what follows nonetheless demonstrates how the divergent data protection legislations of the European Union (EU) and the United States correspond to broad dignitarian and narrow utilitarian privacy conceptions, respectively. Kenya's DPA derives from the EU's 'opt-in' model. Here, before a data processor shares personal information, a data subject's prior informed consent is required. Part 4 traces major decisions of the Kenyan judiciary regarding big data, initially espousing a broad privacy approach. Subsequently, in *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 Others*,[11] the Court of Appeal reverted to a narrow approach that introduces a chilling effect on individual liberty. The LSK thus sought to overturn that decision. However, the Supreme Court rejected LSK's claim, since it was neither a party before the superior nor before the appellate court. This article argues that LSK's impugned appeal arguably reflects an alternative privacy conception that does not focus on the benefit of the individual or of preventing interference, inconvenient or private disclosures 'but on the benefits to society, of maintaining a sphere of life insulated from the public gaze'.[12] Part 5 thus considers the benefits of group privacy which LSK's dismissed appeal set out to prioritise. The article concludes that African culture may proffer group privacy over the value of individualised human dignity emphasised not only in Kenya's DPA, but also international instruments, including the Draft Legal Instrument on Government-led Surveillance and Privacy (LIGSP) of the United Nations (UN).[13]

2 Surveillance ethics

2.1 Intelligence and surveillance

No agreed definition for state intelligence exists.[14] It has been defined as information theft. On the one hand, private theft is universally disapproved of as violating the moral code and thieves are subjected to savage sanctions. On the

10 Chesterman (n 7) 243.
11 [2020] eKLR (the *Mobile Telephones* case).
12 Chesterman (n 7) 244.
13 Draft Legal Instrument on Government-led Surveillance and Privacy 10 January 2018 (LIGSP), DraftLegalInstrumentGovernmentLed.pdf (accessed 31 January 2023).
14 D Omand & M Phythian *Principled spying: The ethics of secret intelligence* (2018) 9.

other hand, such information-gathering contrary to an owner's will is deemed permissible to detect and thwart threats to others or to the state, that is, to enhance public safety and national security.[15] Surveillance has two justifications. Internationally, states are suspicious about one another's intentions. Therefore, given the anarchic global legal order, surveillance is justified by neorealist international relations theory.[16] Domestically, Hobbes' *raison d'ȅtre* of the liberal nation state deems that individuals should surrender some personal autonomy to a centralised authority, responsible for public security, law and order. However, Rousseau's social contract displays tension between being human and becoming citizens. The latter are able to acknowledge in themselves and others the common conditions of being human and, thus, are willing to join with others on that footing of the common.[17] However, some individuals are free riders. Without the compulsion of law, they are incapable of remaining loyal to the sovereign. Ignoring all the duties incumbent on citizens, such self-interested individuals try to benefit from citizenship without paying the price. Thus, to obey the general will, Rousseau suggests that unwilling subjects should be 'forced to be free'.[18] For Weber, the state's administrative staff therefore possesses a monopoly over legitimate violence to enforce the political order.[19]

Rebels and criminals breaking rules challenge the prevailing constitutional arrangement's legitimacy.[20] Yet, relying on physical restraint by the police, prosecutors, judges, lawyers and jail wardens combining with prison apparatuses to repress reprisals is prohibitively expensive or even counterproductive.[21] Moreover, rather than relying on uninformed opinions of the lesser informed citizenry, the gathering of accurate information is instrumental to maintaining peace and security. People who are better informed are required to anticipate potential risks and actual threats to others and the state. Therefore, in order to prevent harms and prosecute crimes, governments are justified in establishing agencies to collect secret intelligence.[22] However, because the substantive right to privacy is primary, the executive is procedurally constrained to seek judicial evaluation of the quality of evidence against any suspect whose home is to be searched, possessions seized, family information required or communications intercepted. It is important to acknowledge data protection as a procedural right, providing regulations, methodologies and conditionalities by which substantive privacy and identity rights are effectively enforced.[23] In liberal democracies, privacy remains paramount. Hence, warrantless searches are prohibited.[24] Unless

15 Omand & Phythian (n 14) 10.
16 Omand & Phythian (n 14) 11.
17 TB Strong *Jean-Jacques Rousseau and the politics of the ordinary* (1994) 76.
18 J-J Rousseau *The social contract: Book I* (1895) chs 6-9.
19 Omand & Phythian (n 14) 14.
20 Omand & Phythian (n 14) 15.
21 WH Riker 'Public safety as a public good' in EV Rostow *Is law dead?* (1971) 383.
22 Omand & Phythian (n 14) 16.
23 NNG de Andrade 'Oblivion: The right to be different ... from oneself: Re-proposing the right to be forgotten' in A Ghezzi, AG Pereria & LV Alujevic (eds) *The ethics of memory in a digital age: Interrogating the right to be forgotten* (2014) 66-67.
24 Sec 29 Criminal Procedure Code (Chapter 75 Laws of Kenya).

the threshold of reasonable suspicion of criminality is attained, courts are not justified in issuing search warrants. By providing the minimum information needed by those who have to make security and public safety decisions, secret intelligence still plays a significant part in eliciting evidence for the criminal justice system.[25]

2.2 The chilling effect of warrantless mass surveillance

Mass surveillance inhibits people from freely expressing their thoughts, giving rise to self-censorship or creating a chilling effect. Upon becoming aware, either that they are being watched or that they are possibly watched, people also become frightened. Since they are afraid of the possible consequences of surveillance, they tend to avoid it altogether. Hence, they fear exercising their liberty of acting on their thoughts. Making people live under a cloud of anxiety violates privacy and offends dignity. The need to prohibit such chilling is evident in a line of European Court of Human Rights decisions. For instance, if a lawyer is required to report on his client's sources of money, as recommended under a Proceeds of Crimes and Money Laundering Act, then he simultaneously fears being struck off the roll of advocates or facing disciplinary proceedings for breaching advocate-client confidentiality. Consequently, even before any precipitate action has yet befallen him, he has a right to challenge such chilling legislation. Although he lodges a hypothetical court action to prevent future harm, in Europe such anxious lawyers have been held to fulfil the victim requirement.[26] Similarly, the Court has held that in Amsterdam, where certain zonal areas were subjected to surveillance, fearful people have the limited options of either frequenting them and exposing themselves to randomised searches or avoiding them altogether. By creating a chilling effect, such self-restraint violates privacy.[27] This principle extends to surveillance on the internet, whether through eavesdropping, hacking or wiretapping. The chilling effect it creates forces people to avoid using electronic media for communication for fear of having their locations detected or communications intercepted. Consider section 36 of Kenya's National Intelligence Service Act (NISA). It provides that: '[t]he right to privacy set out in article 31 of the Constitution may be limited in respect of a person suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with'.[28] Furthermore, under section 42, '[w]here the Director-General has reasonable grounds to believe that a warrant under this section is required to enable the service to investigate any threat to national security or to perform any of its functions, he or she may apply for a warrant'.[29]

25 Omand & Phythian (n 14) 16-17.
26 *Michaud v France* Application 12323/11 (6 December 2012).
27 *Colon v The Netherlands* [2012] ECHR 946.
28 Sec 36 National Intelligence Service Act 28 of 2012.
29 Sec 42 National Intelligence Service Act.

Similarly, the Prevention of Terrorism Act (PTA)[30] contains unique procedures permitting targeted wiretapping for intelligence. Where there are compelling reasons for gathering data of the perpetration of a terrorism-related crime, a High Court judge may authorise wiretapping. A chief inspector of police may make a self-interested application requiring power to intercept communication. Nonetheless, dangers of generalised snooping are adequately addressed by not only requiring the police inspector-general's or the director of public prosecutions' written consent, but also imposing 10 years' imprisonment or a Kenya shilling 5 million fine (USD $ 30,800), or both, on officers who engage in wiretapping contrary to judicial authorisation.

3 The socio-ethical and legal framework of the right to privacy

3.1 Social ethical norms of privacy

Privacy establishes a niche in which individuals have the liberty to choose how they think and act. Under liberal democratic ethical and legal values, without their own informed consent, no one should be manipulated to disclose personal information about themselves to others. On the continental European variation, freedom means that when in private and public, individuals need not maintain an identical persona. Rather, one may choose to be reserved, shy and self-centred in private, yet portray an outgoing and caring public image.[31] No one should be compelled to reveal their true inner selves to others, whether concerning their mental or physical health, age, weight, attitudes, perspectives, political preferences, sexual orientation, or all and sundry matters. Personal freedom, autonomy and human dignity are fostered in the private sphere. Therefore, to enhance spiritual nature, feelings and intellect, individuals should easily express thoughts without apprehension that unwanted ears or eyes, including the government, are listening in or prying on them. An emergent chilling effect arises upon invading privacy, eroding the good life to the detriment of happiness.[32]

Privacy scholars have shown that, in liberal constitutions, one merit of privacy's social value is that opening the emotional and physical sphere in which ideas can be formulated, incubated and evaluated, fosters society's intellectual gestation.[33] Nonetheless, in Kenya, as shown in part 4.2 below, attempts to develop a privacy jurisprudence by striking down state encroachment into social space through surveillance overreach under the guise of providing national security, have been reversed on appeal. There is tension between individual privacy rights and collective security interests. While liberal democratic society as a whole is better off

30 Sec 36 Act 30 of 2012.
31 ED Cohen *Technology of oppression: Preserving freedom and dignity in an age of mass, warrantless surveillance* (2014) 3.
32 As above.
33 R Jay *Data protection law and practice* (2007).

if it facilitates the development of autonomous individuals, the state is mandated to provide collective security and requires information for that purpose. On the one hand, right to privacy proponents contend that opinions and ideas may lead to scientific, artistic and technological or political contributions from which all may benefit.[34] From this perspective, prerequisites to the development of ideas and nurturing of beliefs to develop self-confidence entail the needs to cultivate private spaces for reading, thinking, and confidential communications away from the interference of others.[35] Presumably, private citizens cannot tolerate excessive state intrusion into their lives. Therefore, by requiring the police to prove reasonable suspicion in order to obtain court warrants to search for a specific crime, conditional protections prohibit privacy invasion. Indeed, surveillance is not security and should be impartial.[36]

Is the use of generalised surveillance constitutionally permissible or does it violate privacy rights? For Nwauche, the modern right to privacy has received little legal attention in Nigeria. This creates the false impression that Nigerians can dispense with their privacy.[37] Abdulrauf thus concurs that a more effective framework is needed to protect individuals from new technological threats that have the capacity to denude one's command regarding an important component of their own personality and personal information.[38] By derogating from privacy rights, subject to requiring public participation to ratify such surveillance, Kenyan courts upheld an amendment to the 2012 PTA through introducing section 36A under the Security Laws (Amendment) Act (SLAA) for interception of private communications in the war on terrorism. More recently however, in the *Mobile Telephones* appeal, the Court seemed oblivious to the notion that generalised surveillance of disenchanted groups stifles education, personal identity and democracy that flourish in private.

Most privacy notions focus on broad individual dignity claims or narrow utility needs, rather than group privacy. For example, libertarian Mill stated that 'the only part of the conduct of anyone, for which he is answerable to society, is that which concerns others. In the part which merely concerns him, his independence is, of right, absolute.'[39] Over oneself, over their own body and mind, each person is sovereign.[40] Numerous theorists conceptualise privacy as

34 K Hughes 'The social value of privacy, the value of privacy to society and human rights discourse' in B Roessler & D Mokrosinska (eds) *Social dimensions of privacy: Interdisciplinary perspectives* (2015) 226, 229.
35 Hughes (n 34) 229.
36 B Wittes & G Blum *The future of violence: Robots and germs, hackers and drones: Confronting a new age of threats* (2015).
37 ES Nwauche 'The right to privacy in Nigeria' (2007) 1 *Review of Nigerian Law and Practice* 63.
38 LA Abdulrauf 'New technologies and the right to privacy in Nigeria: Evaluating the tension between traditional and modern conceptions' (2016) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 120-122, 124.
39 A Dix and others 'EU data protection reform: Opportunities and concerns' (2013) 48 *Intereconomics* 268-285.
40 L Floridi 'Group privacy: A defence and an interpretation' in L Taylor, L Floridi & B van der Sloot (eds) *Group privacy: New challenges of data technologies* (2016) 83-100.

'limited access' to the self. Such notion affirms each person's desire for secrecy and for being isolated from others.[41] Consent is key. However more broadly, according to Westin, 'privacy is the claim of individuals, *groups*, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[42]

3.2 Constitutional and statutory basis for regulating big data

3.2.1 Legal positivism

Privacy of individuals under the Kenyan Constitution guarantees that –

> Every person has the right to privacy, which includes the right not to have –
>
> (a) their person, home or property searched;
> (b) their possessions seized;
> (c) information relating to their family or private affairs unnecessarily required or revealed; or
> (d) the privacy of their communications infringed.[43]

To undergird this constitutional privacy protection, Parliament enacted the DPA. It reinforces compliance with the country's international obligations.[44] Such treaties include the Universal Declaration of Human Rights (Universal Declaration)[45] and International Covenant on Civil and Political Rights (ICCPR),[46] which enshrine privacy rights. They are domesticated into Kenyan law under the opening chapter on 'Sovereignty the people and supremacy of this Constitution' which states that '(5) [t]he general rules of international law shall form part of the law of Kenya.' Further '(6) [a]ny treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution.'[47] However, under the Bill of Rights, article 24 specifically states that privacy is not absolute. Altogether, the statutory privacy clauses have some shortcomings, including ineffectively and inadequately protecting personal data.[48]

41 DK Mulligan, C Koopman & N Doty 'Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy' (2016) 374 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, http://dx.doi.org/10.1098/rsta.2016.0118 (accessed 26 January 2022).

42 G Bhatia 'State surveillance and the right to privacy in India: A constitutional biography' (2014) 26 *National Law School of India Review* 127 (my emphasis), http://www.theregister.co.uk/2013/05/08/india_privacy_woes_central_monitoring_system/ (accessed 14 February 2023).

43 Art 31 Constitution of Kenya (Government Printer 2010).

44 M Laibuta 'The data protection officer' (2020), https://www.laibuta.com/data-protection/the-data-protection-officer/ (accessed 16 February 2023).

45 Adopted by General Assembly Resolution 217 A(III) of 10 December 1948.

46 Adopted by the United Nations General Assembly Resolution 2200A (XXI) of 16 December 1966.

47 Art 2 Constitution of Kenya.

48 N Kagotho 'Towards household asset protection: Findings from an inter-generational asset transfer project in rural Kenya' (2020) 7 *Global Social Welfare* 23.

3.2.2 Dignitarian rights theory

As alluded to above, the global commitment to human dignity is immortalised by the Universal Declaration. According to Gathii, the Universal Declaration represents 'the single most important reference point for cross cultural discussion of human freedom and dignity in the world today'.[49] Because everyone is born free and equal in dignity and rights,[50] article 22 proclaims that each member of society is entitled to the realise 'economic, social and cultural rights indispensable for his dignity and the free development of his personality'. Furthermore, the Constitution's article 28 upholds the right to have one's inherent 'dignity respected and protected'.[51] Thus, the dignitarian rights theory formulates privacy as an inalienable and sacred right that should not be derogated from. Dignity entails notions of honour to the privacy right. Hence, its safeguard attaches an intangible non-economic interest.[52] It is mostly developed in the theory of privacy protection of the dignity and moral autonomy of the human subject. Specifically, 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation'[53] and 'everyone has the right to the protection of the law against such interference or attacks'.[54]

3.2.3 Consequentialist ethical theory

Consequentialist ethical theory is predicated upon the capability to anticipate the consequences of an action.[55] Utilitarians are one category of consequentialists. To utilitarians, the choice that is ethically correct is the one that yields the greatest happiness to the majority. Unlike the dignitarian rights theory, utilitarianism seeks to protect an interest as opposed to the protection of a right. Generally, utilitarian ethics does not recognise privacy as an independent value, deserving of protection in its own right. Act and rule utilitarianism are two main utilitarianism types.[56] Act utilitarianism propounds the above utilitarianism definition precisely. Irrespective of personal sentiments or the societal constraints such as laws, an individual performs the act that confers profits on the majority. Conversely, rule utilitarianism also seeks surplus value for the majority, but using the fairest and most just means available. Therefore, it values justice and includes some benefit.[57] In Rawls's view, rule utilitarianism is the better ethical principle

49 JT Gathii 'Jurisdiction to prosecute non-national pirates captured by third states under Kenyan and international law' (2011) *SSRN Electronic Journal*, http://digitalcommons.lmu.edu/ilr/vol31/iss3/2 (accessed 9 February 2023).
50 Art 1 Universal Declaration(n 45) .
51 Art 28 Constitution of Kenya.
52 J Bonnitcha 'The implications of the structure of the regulatory expropriation enquiry in international investment law' MPhil dissertation, University of Oxford, 2008.
53 Art 12 Universal Declaration(n 45) .
54 Art 17(2) ICCPR(n 46) .
55 H Delany, E Carolan & C Murphy *The right to privacy: A doctrinal and comparative analysis* (2008).
56 SD Warren & LD Brandeis 'The right to privacy' (1890) 4 *Harvard Law Review* 193-220.
57 AM Lusambili & others 'Deliver on your own: Disrespectful maternity care in rural Kenya' (2020) 15 *PLoS ONE*.

to follow, as within the confines of justice to all, it promotes the greatest good for the greatest number of people.[58]

4 Alien origins of data protection legislation

4.1 Europe

Western continents on both sides of the Atlantic display divergent privacy cultures. Their respective sensibilities spawn different laws. The EU's 'command and control' model governs the handling of personal information with precise rules. A prominent governmental involvement protects the consumer's privacy. Such culture is perfectly acceptable, since Europeans valorise privacy to protect human dignity.[59] An EU Directive demands that personal data must not only 'be processed fairly and in a manner consistent with specified, explicit and legitimate purposes, maintained accurately, updated periodically, erased or rectified in a timely manner'. It must also be 'kept anonymously when identification of data subjects is no longer necessary'. Only when 'the data subject has unambiguously given his consent', may processing take place.[60] Making data processing dependent on the individual involved, and requiring a subject to express consent, adopts an 'opt-in' standard. Someone's political, religious, racial, or ethnic extraction, health status and union membership are among types of information that cannot be processed without explicit consent. Unless data controllers give their targets even more protection, the data can be erased. They should not only supply the reason – for the processing, who shall perceive the data, and specify the rights that the subject is entitled to – but also take appropriate security measures.[61] The Directive further requires member states to ensure that any personal information transmitted to a third country depends on reciprocal protection levels. Compliance is contingent upon numerous criteria ranging from the nature of information, to the legal rules prevalent in the recipient country, to the protective measures undertaken.

4.2 The United States

Free speech facilitates searching for truth. The US Constitution's First Amendment thus prohibits Congress from abridging expressive freedom.[62] This approach gives subjects a chance *not* to 'opt in' to data processing. It incorporates an 'opt-out' protocol, where individuals need to actively block collection or

58 J Rawls *A theory of justice* (1971).
59 Donoghue (n 6) 206.
60 Donoghue (n 6) 207.
61 Donoghue (n 6) 208.
62 JM Boland 'Is free speech compatible with human dignity, equality, and democratic government: America, a free speech island in a sea of censorship' (2013) 6 *Drexel University School of Law* 1-46.

commercial utilisation of personal information about themselves. Nonetheless, privacy culture stems from liberty. While security has historically been entrusted to the police, a premium is placed on preserving both individual autonomy and commercial flexibility. Consequently, self-policing supports the internet's continuing evolution and development.[63] At federal level, no comprehensive legislation is enacted to regulate data gathering and information use. Instead, the US industry combines self-regulation with governmental restraint towards dealing with information in the possession of third parties. Distinctly lower protections accorded to personal information in the US means that European entities may be prohibited from transmitting information to US actors. Therefore, under the Safe Harbor Agreement, reasonable precautions must be undertaken by US companies to ensure that data integrity information transferred from the EU to 'Safe Harbor' companies should continue without special approval.[64]

Inspired by Westin's US-based taxonomy, the present-day debate concerning online privacy typically depicts privacy as a good to be exchanged with other commodities.[65] This classification divides the privacy population into three: the fundamentalists, the pragmatics and the unconcerned. Europeans are privacy fundamentalists. They are sticklers for the highest, and consequently a utopian, standard of privacy safeguards.[66] The US are privacy pragmatics. They consent to a continuous erosion of privacy to accommodate expediency. Africans are the privacy unconcerned. They pay scant heed about their personal information. This framing serves the interests of those who profit from piercing the privacy veil. It assumes either that Africans are unconcerned about privacy or that they invest more in communal values. However, this hardly leaves room for a more flexible perspective of what constitutes group privacy and its aims. Given that all privacy essentially concerns managing boundaries along both space and informational dimensions, as some theorists suggest,[67] it is critical to grasp how such boundaries are managed within the digital domain, considering its unique substance and informational characteristics in relation to security requirements.

63 Donoghue (n 6) 208.
64 As above, 209.
65 Kagotho (n 48).
66 C Staunton and others 'Protection of Personal Information Act 2013 and data protection for health research in South Africa' (2020) *International Data Privacy Law*, https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipz024/5715399 (accessed 16 February 2023).
67 Z Tufekci 'Can you see me now? Audience and disclosure regulation in online social network sites' (2008) 28 *Bulletin of Science, Technology & Society* 20-36; DM Boyd & NB Ellison 'Social network sites: Definition, history, and scholarship' (2007) 13 *Journal of Computer-Mediated Communication* 210-230; GH Lapenta & RF Jørgensen 'Youth, privacy and online media: Framing the right to privacy in public policy-making' (2015) 20 *First Monday*, https://journals.uic.edu/ojs/index.php/fm/article/download/5568/4373 (accessed 14 February 2023).

4.3 Kenya's Data Protection Act

Reinforcing the constitutional provisions on privacy and informational rights, protection from the misuse of personal information is impliedly legislated in Kenya. Insisting on a trajectory of clear affirmative action, the DPA provides that the data subject's 'consent' to the processing of personal data must be an express, unambiguous, free, specific and informed expression of the data subject's desires. Apparently, to process personal data, controllers and processors are precluded from invoking implied consent.[68] However, whether or not a corporation may be able to invoke pre-ticked boxes or any other 'opt-out' consent by default, or whether a positive 'opt-in' mode shall suffice, is less clear. Hence the need for data controllers and processors alike to rethink their contemporary consent practices. 'Sensitive personal data' is more broadly defined to include proprietary particulars, marital status and family relationships, including names of the individual's parents, or spouse(s).[69]

In the application for registration, the DPA specifies the information to be supplied by the data controller and processor. They must attain adequate and minimal safeguards, security thresholds and modalities. However, this obligation is mitigated by the quantity of personal data gathered, the processing costs, and the scope of processing dynamics. Included among the application demands is a novel provision so that applicants should specify what methods are devised to indemnify data subjects from unlawful use.[70] The indemnification conditionality also signifies that data controllers and processors must account for any trespass on a data subject's rights and interests in personal data. Common data protection principles are embodied in data protection legislation worldwide. Domestically, section 25 of the DPA resembles principles applicable to international standards,[71] particularly the EU's General Data Protection Regulation (GDPR).[72]

Any individual processing the personal data of a subject is obligated to incorporate acceptable techniques for verifying age and determining consent. The selection of mechanisms may be influenced by the available technology, the ratio and the quantum of such personal data to probably be processed. A data audit, dubbed a data protection impact assessment (DPIA), may facilitate a determination of whether or not specific activities should be implemented before gathering or processing any individual's data. Where there is a 'real risk of harm'

68 G Greenleaf & B Cottier '2020 ends a decade of 62 new data privacy laws' (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=357261 (accessed 16 February 2020).
69 BJ Koops 'The trouble with European data protection law' (2014) *International Data Privacy Law* 1-14, http://idpl.oxfordjournals.org/ (accessed 9 February 2023).
70 L Determann & C Gupta 'Indian Personal Data Protection Act, 2018: Draft Bill and its history, compared to EU GDPR and California privacy law' (2018) SSRN *Electronic Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3244203 (accessed 26 March 2023).
71 Koops (n 69).
72 Repealing Directive 95/46/EC (Data Protection Directive), https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (accessed 27 March 2023).

to the data subject whose personal data has been acquired by an unauthorised person accessing their data, the DPA prescribes the response to be taken.[73]

5 Big decisions regarding big data

5.1 Early cases

5.1.1 The *Security Laws Amendment Act* case

In February 2015, in *Coalition for Reform and Democracy (CORD) & Another v Republic of Kenya & Another*,[74] the official opposition coalition led petitioners challenging the Security Laws (Amendment) Act's attempt to introduce section 36A to the PTA, which proposal stated that the national security organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism. Furthermore, it provided that where they aim to intercept such communication, the Constitution's article 31 privacy right shall be limited.[75]

This amended provision was designed to limit the privacy right. It aimed to introduce unprecedented mass surveillance of communication by the national security agencies. Hence, its constitutionality was challenged. The state's rebuttal was that surveillance is justified in the war on terror.[76] The Constitutional Court observed that 'by widening threats of constant exposure, thus allowing intruders to pry on their personal space', surveillance 'in terms of intercepting communication jeopardises the petitioner's privacy'.[77] Nonetheless, given the scores of terrorist attacks in Kenya's recent past, the impugned provision was of genuine public interest. The privacy right, therefore, had to be balanced against common good exigencies.[78] All five judges concurred that there were sufficient safeguards ensuring that the limitations placed on privacy rights by intercepting communication and conducting searches would not be undertaken arbitrarily and using a widespread scope.[79] Consequently, limiting privacy was upheld as justified in a free and democratic society, for detecting, disrupting and preventing terrorism.[80] Simultaneously, in an apparent bid to stem the tide of generalised surveillance, SLAA amended section 36 of NISA to permit warranted derogations from privacy during investigations and monitoring of a person 'who is subject to investigation by the service'.[81] Ironically, however, immediately after this case,

73 Staunton and others (n 66).
74 [2015] eKLR.
75 *CORD* (n 74) 55-56 para 65. It introduced sub-secs 36(4), (5) & (6).
76 *CORD* (n 74) 59 para 298.
77 *CORD* (n 74) 57 para 290.
78 *CORD* (n 74) 60 para 302.
79 *CORD* (n 74).
80 *CORD* (n 74) 61 para 308.
81 Sec 55 Security Laws (Amendment) Act 2014.

as demonstrated in part 5.2.2 below, a broad privacy approach was adopted by courts constraining data collecting and monitoring. Only recently have the courts reverted back to a narrow approach permitting generalised surveillance and, thus, failing to avert big data's chilling effect.

5.1.2 The *Nubian Rights Forum* case

In *Nubian Rights Forum & 2 Others v Attorney General & 6 Others; Child Welfare Society,*[82] several organisations complained against the destruction, deletion or loss of vital records containing personal data, and of identity theft and fraud. They expressed fear of malicious utilisation of the information, false entries, mismatching information and hacking through cybercrimes. High Court justices Ngugi, Nyamweya and Korir JJ (as they then were) agreed that the state's proposed DNA collection and global positioning system (GPS) co-ordinates for identification purposes were invasive, unnecessary, and unauthorised by the impugned enabling legislation. Because data protection was not guaranteed, the scheme violated the Constitution's article 31 privacy rights.

5.1.3 The *HIV* case

In 2015, President Uhuru Kenyatta ordered all county commissioners and three cabinet secretaries for the Ministries of (i) Interior and Coordination of Government; (ii) Education, Science and Technology; (iii) Health; as well as (iv) the National AIDS Council, to gather updated data and report on all school-going children living with HIV and AIDS.[83] However, four petitioners were apprehensive, first, that in violation of the HIV and AIDS Prevention and Control Act,[84] the order would result in forced or compulsory testing, second, that it would also result in forced disclosure of information about one's HIV status, contrary to privacy rights, equality freedoms, as well as the targeted persons' dignity.[85] The respondents rebutted by saying that the President's impugned directive aimed to provide HIV-positive persons and the private sector with necessary political will. Furthermore, that this data would also increase limited access to anti-retrovirals (ARVs) for school-going children and youths who suffer stigma and exclusion for living with HIV.[86] Moreover, several guidelines provide for privacy and confidentiality in implementing services, research and data gathering in different situations.[87] Indeed, they countered that the names of people with chronic care conditions, not only persons living with HIV, are already available in respective hospital and HIV care clinic registers, for

82 [2020] eKLR (*Nubian Rights Forum* case).
83 *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v Cabinet Secretary Ministry of Health & 4 Others* [2016] eKLR.
84 14 of 2006.
85 *KELIN* (n 83) para 14.
86 *KELIN* (n 83) para 30.
87 *KELIN* (n 83) para 32.

follow up, attention and ARV treatment.[88] However, a UN expert reinforced the petitioners' perspective that the unlawful disclosure of an individual's HIV status contravenes their privacy rights.[89]

Defining privacy to include 'those matters whose disclosure will cause mental distress and injury to a person', Lenaola J (as he then was), approaching privacy broadly, held that the Constitution's article 31(c) protects against the unnecessary revelation of information regarding family or private affairs.[90] Articulating privacy as a right to live one's own life with minimum interference, he held that it also restricts the gathering, utilisation and disclosure of private information.[91] Consequently, the judge struck down the directive as unconstitutional. It violated the petitioners' constitutional privacy rights and as such was not in the child's best interests. Instead, he ordered that the children's names should be stored in a public document in a way that delinks their HIV statuses from themselves.

5.2 The *Mobile Telephones* case

5.2.1 The High Court

In April 2018, in *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others*[92] the High Court held that phone records should not be deployed for generalised surveillance. Mativo J (as he then was) approached privacy as a broad fundamental human right that is 'central to the protection of human dignity and forms the basis of any democratic society'.[93] Yet, this article notices that nowhere is any right to privacy expressly enshrined in the African Charter on Human and Peoples' Rights (African Charter). It is only implied by the collective self-determination right.[94] Nonetheless, the judge recognised that domestically '[t]he right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals'.[95] Therefore, surveillance and censorship that restrict privacy may only be justifiable when 'prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued'.[96] Furthermore, the emergence of new challenges is exemplified by the context of an information based world. The judicial task in the information era, where technology infiltrates almost every dimension of our activities, is to

88 *KELIN* (n 83) para 33.
89 *KELIN* (n 83) paras 43-50.
90 *KELIN* (n 83) para 68.
91 *KELIN* (n 83) para 69.
92 [2018] eKLR.
93 *Okoiti* (n 92) 16 para 63.
94 V Bermingham, J Hodgson & S Watson *Nutshells tort* (2014).
95 *Okoiti* (n 92) 16 para 63.
96 As above.

confer constitutional meaning to individual liberty in the global network. Kenya's Constitution protects privacy as a basic principle. Consequently, in a digitised world the court should be responsive to the necessities of surveillance abuse and the possibilities and risks to liberties.[97]

Mativo J declared that since the mobile network owners were excluded from consultations in policy formulation and implementation, the government's intended telephone surveillance policy was constitutionally invalid as it conflicted with the right to privacy. He agreed with Okoiti that by installing a communication surveillance system, styled as the 'device management system' (DMS), on mobile telephone networks, 'millions of subscribers and the general public whose records are held' were endangered. Clearly, to monitor the population by defying the constitutional protection of privacy, the government had a hidden agenda. To Okoiti's chagrin, the DMS device would spy or snoop on the general population and harvest and stock subscribers' personal data. This would facilitate the state's access, collection and retention of subscribers' communication data. However, according to the Communications Authority of Kenya (CAK), the DMS system was meant to fight fake and offending devices. Ultimately, the High Court prohibited CAK from effecting its decision to establish connectivity between the DMS and mobile phone operators.[98]

5.2.2 The *Mobile Telephones* case: Court of Appeal

In *Communications Authority of Kenya v Okoiti & 8 Others*[99] the CAK successfully appealed. Ouko J (as he then was), Koome (afterward Chief Justice) and Musinga JJA considered three issues: first, whether by intercepting and recording of communication and mobile data, the DMS installed by CAK would signal an era of public regulation and espionage on peoples' privacy; second, whether the CAK adequately allowed public participation in the development and installation of the DMS; third, whether the dispute was prematurely taken to court.[100] They recalled that 'since its advent in Kenya in early 2000', the regulation of mobile communication 'was guided by the world-wide global system for mobile communication (GSM)'. Because Kenya agreed, by various international agreements, 'to identify mobile communication devices that have been manufactured with regard to GSM standard', this process is regulated. Therefore, mobile phones must bear a 15-digit serial number called the international mobile equipment identity (IMEI). Such identification mark of quality 'is issued by Global System for Mobile Communications Association (GSMA) which maintains a global central database containing numbers of millions of mobile devices, ie mobile phones, tablets, data cards etc known as IMEI Database'.[101]

97 *Okoiti* (n 92) 16 para 64.
98 *Okoiti* (n 92) 38 para 163.
99 *CAK* (n 11).
100 *CAK* (n 11) 2 para 1.
101 *CAK* (n 11) 2 para 3.

Moreover, world over the theft of mobile handsets and the proliferation of fake and illegal phones came into sharp focus for regulators. Simultaneously, pawns handling counterfeit handsets became more tech-savvy and began cloning genuine IMEI numbers to the dud models, which made discovery more difficult.[102] Consequently, when compared with the GSMA IMEIs database whitelist and in the event of disconnection, counterfeit devices looked legitimate.[103] CAK also faced escalation of SIM boxing, the next horizon for combating fake devices.[104] Effectively, in contravention of section 24(1) of the Kenya Information and Communications Act,[105] SIM boxing operators evade licence fee payments which require that they also do not pay the requisite taxes for eliminating international traffic within Kenya, thus inflicting considerable revenue losses of national capital. The only records that are held by the local operators from a call originating from SIM boxing is the domestic number used in the operations, making SIM boxing a fulcrum for criminal enterprises as the actual source of the audio calls is untraceable. Additionally, CAK received complaints from country operators within East Africa, particularly Rwanda, that the SIM boxing operation in Kenya was being utilised to stop international traffic, causing revenue losses.[106]

CAK's appeal succeeded on technicalities. Procedurally, because Okoiti's petition consisted of 'generalised allegations' that were 'wholly predicated on unsubstantiated statements taken from newspaper reports and statements made by unnamed technical experts'. It was 'slovenly drawn'. In pertinent part, the petition alleged that the state mentioned nothing concerning the system's potential for tapping telephone calls and texts and also peeping into all mobile cash transfers and how it will safeguard individual privacy, once the information is not only gathered by CAK but also hived off by third parties, not limited to the state's law enforcement and other public actors.[107]

Okoiti's rejected evidence comprised newspaper snippets with exaggerated headlines, such as 'Bold plan to spy on all calls, texts rolled out from Tuesday next week, if mobile firms comply, someone other than your provider will be able to access your call, text and money transfer data';[108] and also 'Big Brother could start tapping your calls, texts from next week'.[109] Altogether, Okoiti's supporting depositions on accusations of what scared him may occur, were conjectures or, at best, unconfirmed sources of information. For example, his petition at paragraph 9 speculated that '[t]echnical experts have pointed out that while there would be no concern over the access to the International Mobile Subscriber Identity, which is a unique number identifying a mobile phone subscriber, other access like

102 *CAK* (n 11) 2 para 5.
103 *The Standard* cited in *Okoiti* (n 11) 2-3 para 5.
104 *CAK* (n 11) 3 para 5.
105 2 of 1998.
106 *CAK* (n 11) 3 para 6.
107 *CAK* (n 11) 15 para 37.
108 *Daily Nation* 17 February 2017.
109 *CAK* (n 11) 15 para 38.

home location register raise concerns'.[110] Therefore, the appellate judges allayed his apprehension that the state's motive was to engage in espionage.

In sum, allegations of surveillance abuse by unscrupulous mobile operators also required to strike a balance between securing the privacy right without infringing it.[111] Consequently, the appellate judges unanimously concluded that 'there was no concrete evidence that the DMS was going to spy or intrude on private communication' and, moreover, 'that there were genuine issues raised by MNOs which were still being discussed'. The Court of Appeal ordered, first, that pursuant to its commission of developing a DMS system, the CAK should not halt ongoing consultations among stakeholders and MNOs in order to finish 'the technical and consumer guidelines on the DMS'; second, that such 'guidelines/ regulations should be subjected to public participation'.[112]

5.2.3 The *Mobile Telephones* case: The Supreme Court

Despite the Court of Appeal judges ignoring the DMS constitutionality issue and its threat to privacy rights of millions of mobile telephone subscribers, the Supreme Court faulted LSK.[113] Moreover, it also ignored alarm bells sounded by telephony giant Safaricom that the DMS will enable the CAK to monitor other customer data held by the telecoms operators. Conversely, insisting that the monitoring devices can only find and save the special identification number of mobile devices and assigned subscriber numbers, CAK emphatically denied that the technology had the capacity to access the phone records, locations, and mobile cash transfer particulars of subscribers. Yet, given that LSK was alien to both the High Court and Court of Appeal proceedings, Mwilu DCJ, Ibrahim, Wanjala, Ndung'u and Lenaola SCJJ declined to deal with substantive issues concerning its challenges to data protection law. Neither had Okoiti appealed to the Supreme Court. Therefore, what the apex judges' opinions on the merits may have been, remains moot. Miffed by the order of costs made against it while desperately seeking to execute its own statutory mandate to 'uphold the Constitution and administration of justice', LSK moved to the East African Court of Justice. The advocate's body 'complained over the Supreme Court decision to exclude participants who are not parties to a case from lodging an appeal'.[114] Meanwhile, other civil society activists remained unimpressed with the Court of Appeal's controversial decision and are exploring alternative means of circumventing it.

110 *CAK* (n 11) 16 para 39.
111 *CAK* (n 11) 19 para 47.
112 *CAK* (n 11) 21 para 54.
113 S Kiplagat 'Regulator allowed to install mobile phone spying gadget' 28 April 2023, https://www.businessdailyafrica.com/bd/economy/regulator-allowed-to-install-mobile-phone-spying-gadget--4215610 (accessed 28 April 2023).
114 J Wangui 'Kenya lawyers take Supreme Court to EACJ' *The East African* 26 June 2023, https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-lawyers-take-supreme-court-to-eacj-4282206 (accessed 11 October 2023).

5.2.4 The *Huduma Namba*[115] case

High Court

In *Katiba Institute v Attorney General*,[116] a non-governmental organisation (NGO) challenged the Information, Communications and Technology Cabinet Secretary, Mucheru's 18 November 2019 rollout of a new identity card, known as 'Huduma card', which was proposed as the primary data source on every citizen and foreigner. It was to be issued upon gathering and processing the data subject's personal data.[117] Was such collection and processing of personal data under the National Integrated Identity Management System (NIIMS) subject to DPA?[118] Despite the government having spent more than Sh 10 billion (US $74 626 870) for failing to comply with DPA, Ngaah J nullified the card's launch. Prior to collecting and processing personal data for the Huduma cards, the government should have conducted a data protection impact assessment (DPIA) to identify any risks, such as contraventions to privacy and data loss.[119] Moreover, some Kenyans who lack identity cards may be excluded from the roll-out. Since processing under NIIMS, including the capturing of children's biometrics and data, and was likely to result in high risk to people's rights and liberties, the High Court compelled the state to first conduct the requisite DPIA.[120] Evidently, the judge's decision appears based on promoting board dignitarian privacy concerns. This approach elevated the threshold required to justify societal ouster of privacy rights.

Court of Appeal

In *Attorney General* v *Katiba Institute*,[121] Data Protection Director-General Kassait and Attorney-General Kariuki objected that the Katiba Institute did not possess any data and, thus, was precluded from being an aggrieved person.[122] The Court of Appeal, however, dismissed the government's objection to the hypothetical claim and its plea to continue issuing Huduma Namba cards without conducting impact assessment on data protection. Justices Murgor, Mbogholi-Msagha and Laibuta JJA questioned the state's failure to register Kenyans afresh and conduct a DPIA, as required by DPA. They criticised the government for

115 Swahili for 'service number'.
116 *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 Others; Katiba Institute & Another (Ex parte); Immaculate Kassait, Data Commissioner (Interested Party)* Judicial Review Application E1138 of 2020 [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment).
117 *Katiba* (n 116) 2.
118 *Katiba* (n 116) 3.
119 *Katiba* (n 116) 6-7 para 23.
120 S Kiplagat 'High Court declares Huduma Namba illegal' *Business Daily* 14 October 2021, https://www.businessdailyafrica.com/bd/news/high-court-declares-huduma-namba-illegal--3582926 (accessed 6 March 2023).
121 *Mucheru & 2 Others v Katiba Institute & 2 Others* Civil Application E373 of 2021 [2022] KECA 386 (KLR) (4 March 2022) (Ruling).
122 K Muthoni 'Court dismisses plea to roll out Huduma Namba over data safety' *The Standard* ,https://www.standardmedia.co.ke/national/article/2001439648/court-dismisses-plea-to-roll-out-huduma-namba-over-data-safety (accessed 7 March 2023).

belatedly enacting DPA in the hope of salvaging the Kshs 10.6 billion expended on the data collection exercise. They agreed with Justice Ngaah that the state ought to have first enacted a data protection law, followed by amending the Registration of Persons Act, before rolling out the Huduma Namba exercise. For creatively upholding the activists' hypothetical claims, thereby reverting to a broad privacy approach in departure from Okoiti's *Mobile Telephones* precedent, they endorsed the judge. Kenyan government services are increasingly offered through digital platforms, such as e-citizen. With the proposed new 'Maisha numbers' allocated by the government, national ID cards will gradually be replaced by a transition to digital identity.[123] However, as shown below, just as the theft of Kenyans' irises may expose customers to direct marketing, it is possible that such data, if insecure, may interfere with democratic choices.

5.3 WorldCoin's unauhorised bio-data mining

In April 2023, Data Protection Director-General Kassait discovered that Worldcoin had been collecting personal information from Kenyans. Although Worldcoin had applied for a certificate of registration as a data controller, it neither complied with sections 18 and 19 of the DPA, nor was authorised to operate in Kenya.[124] Yet, hundreds of thousands of Kenyans flocked to the Kenyatta International Convention Centre and several Nairobi malls to have their eye balls captured by parent company, Tools for Humanity and Sense Marketing Limited, traded-off for Kshs 7 000 (US $50) worth of crypto currency.[125] Using their phone application, cryptocurrency and 'orb' scanner, these foreign corporations scanned Kenyans' bio-metric data for over a year. Despite a world class DPA, Worldcoin ignored the DP Commission's instructions to cease invading individuals' privacy by harvesting biometric data, in the absence of proper and convincing justification.[126] It had neither a legal basis for gathering sensitive personal data or the transferring of personal data, nor proof that those people who had their irises scanned had consented to the disclosure of their personal data. Pending the conclusion of investigations, Judge Prof Nixon Sifuna not only prohibited Worldcoin from gathering Kenyans' data, but also ordered it to preserve the information already gathered from 19 April 2022 to 8 August 2023.[127] The hearing continues.

123 Citizen Team 'Gov't to begin Maisha Namba Digital ID awareness drive this weekend' *Citizen* 15 September 2023, https://www.citizen.digital/news/govt-to-begin-maisha-namba-digital-id-awareness-drive-this-weekend-n327456 (accessed 1 November 2023).

124 F Chandianya 'Data commissioner unaware how many Kenyans scanned eyes in Worldcoin' *NTV* 15 August 2023, crazehttps://ntvkenya.co.ke/news/data-commissioner-unaware-how-many-kenyans-scanned-eyes-in-worldcoin-craze/ (accessed 1 November 2023).

125 I Houghton 'Protect Kenyans from digital data trafficking' *Amnesty International* 21 August 2023, https://www.amnestykenya.org/protect-kenyans-from-digital-data-trafficking/ (accessed 1 November 2023).

126 A Njanja 'Worldcoin ignored initial order to stop iris scans in Kenya, records show', https://techcrunch.com/2023/08/15/worldcoin-in-kenya/ (accessed 1 November 2023).

127 S Kiplagat 'Keep off Kenyans' eyes, court orders Worldcoin as probe on' *Business Daily* 15 August 2023, https://www.businessdailyafrica.com/bd/economy/keep-off-kenyans-eyes-court-orders-worldcoin-as-probe-on--4335544 (accessed 1 November 2023).

6 Group privacy, regional and emerging international counter-surveillance and privacy instruments

6.1 Group privacy

Appertaining to big data analytics, it was Floridi who pioneered the group privacy idea.[128] In his thesis, groups have privacy rights that are irreducible to the privacy of individual members of such groups. In response to big data technology advances, group privacy, therefore, should also be a goal of privacy control. Nonetheless, an absolute right, whether of individuals or groups, to *inferential* privacy, is unrealistic.[129] Under a narrow conception, privacy is essential for restricted access to oneself or information about the self, the right to be left alone.[130] In digital interactions, privacy may be understood as an all-embracing right that safeguards virtually every component of identity, personhood and dignity.[131] Because *homo sapiens* as citizens are social beings and, further, because human joy requires that individuals expose their inner selves to one another, therefore, this is a consequentialist approach. Effectively, by joining groups, individuals violate their own privacy and to keep within the group what was revealed, rely on those with whom they associate not to reveal their shared secrets. Such group privacy safeguards people's external, as opposed to their internal, space. This expresses their gregarious nature, rather than their desire for complete isolation.[132] Nonetheless, group privacy remains an individual right. In situations where groups may, nonetheless, be easily identified and targeted, Floridi highlights the risks emerging from opening *anonymised* personal data to public access.[133] Practically, every form of generalised knowledge may subject groups to special risks. Consider the discovery that smoking causes cancer, exposing all smokers to enhanced insurance premiums.[134] Similarly, in virtue of generalised knowledge extracted from a few of a group's individuals, *inferences* about other individuals in the group may be drawn. An entity's individual or collective *inferential* privacy, is a metric of the logically valid inferences, regarding someone's *sensitive features*, that can neither be made nor derived from the available data.[135] Sensitive features 'can be defined as features which most individuals in a given society at a given time do not want widely known about themselves'.[136]

128 L Floridi 'Open data, data protection, and group privacy' (2014) 27 *Philosophy and Technology* 1-3.
129 M Loi & M Christen 'Two concepts of group privacy' (2020) 33 *Philosophy and Technology* 207-224.
130 Warren & Brandeis (n 56).
131 M Hildebrandt 'Balance or trade-off? Online security technologies and fundamental rights' (2013) 26 *Philosophy and Technology* 357-379.
132 EJ Bloustein *Individual and group privacy* (2003).
133 Floridi (n 40) 98.
134 L Taylor 'Safety in numbers? Group privacy and big data analytics in the developing world' in Taylor and others (n 40) 14.
135 Loi & Christen (n 129) 218.
136 Loi & Christen (n 129) 219 citing WA Parent 'Privacy, morality, and the law' (1983) 12 *Philosophy and Public Affairs* 269-288.

An algorithmically-sorted group should, if its members so desire, possess a right to fashion their identity and advance their common interests.[137] It might as well be conceded that individuals in such group may share an interest *not* to be amalgamated into a collective, for example, a group that is discriminated against. However, in such specific society, the group interest in issue is a mere shared interest, an aggregate of identical individual interests. At least in design or in conception, it is not a collective interest in a way that presupposes the prospects of group interaction.[138] Rather, what big data analytics threaten is specifically the *inferential* privacy of individuals that are characterised by sensitive features common to all-inclusive groups. The allegedly special danger facing the *inferential* privacy of groups (compatible with the anonymity of individuals within such groups) may be reduced to a more pervasive difficulty regarding destructive utilisation of generalised knowledge. Such knowledge may affect far more people than the few who facilitated the acquisition of such knowledge.[139] Not all types of privacy can be protected by giving individuals, or groups, rights to regulate information. On the contrary, *inferential* privacy needs a notion of the societal impact of innovation. In this article's argument, invoking rule utilitarianism, LSK's challenge against CAK's generalised surveillance may be seen as objecting to client, patient or customer communications that are in possession of telephone operators, being generally shared with the state by the regulator. Generalised eavesdropping may cause advocates as a group to 'chill' from utilising 'leaky' mobile telephones for fear of breaching ethical duties prohibiting them from divulging client information to third parties without consent.

6.2 Regional comparisons

The African Charter[140] lacks an express privacy right. Nonetheless, privacy may be *inferred* as a derivative of the universal prohibition on arbitrary killing. Locke was of the view that natural laws exist, one of these being the right to life.[141] The Western right to privacy originates in individualism, since each person possesses a right to self-determination. This means that they have the right to choose which aspects of their personal lives to reveal and which aspects to conceal. Conversely, from an African perspective, privacy is perceived as a group right, since '[a]ll peoples shall have the right to existence. They shall have the unquestionable and inalienable right to self-determination. They shall freely determine their political status and shall pursue their economic and social development according to the policy they have freely chosen.'[142] In this context, self-determination is a

137 B van der Sloot 'Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR' in Taylor and others (n 40) 159-173.
138 DG Newman 'Collective interests and collective rights' (2004) 49 *American Journal of Jurisprudence* 140.
139 Loi & Christen (n 129) 222.
140 African Charter on Human and Peoples' Rights concluded at Nairobi on 27 June 1981.
141 Van der Sloot (n 6).
142 African Charter (n 140).

persisting right – one that is not successfully actualised by decolonisation or individualisation and the disappearing of racist regimes. Although the right to secede is not expressly enshrined by the African Charter, it also is not prohibited. Hence, self-determination is exercised by groups, rather than individuals.[143]

Nwauche reflects that, in the Nigerian Constitution, there may be a generalised and specialised understanding of privacy. On the one hand, the provision's general right is 'the privacy of citizens'. Conversely, the phrase 'their homes, correspondence, telephone conversations and telegraphic communications' lists specific instances of the general right. Furthermore, applying principles from the torts of breach of confidence and of privacy,[144] these privacy perspectives create a dilemma, namely, if respect for a private life is defined too widely, it could lead to an undesirable restriction on the freedom of the press to report and comment on matters of public importance. This has concerned English courts.[145] Abdulrauf thus concludes that Nigeria's narrow constitutional provision may be an insufficient legal instrument for individuals to enforce their right to control the access and utilisation of personal information.[146]

6.3 International initiatives

In 1980, a White Paper by Lord Diplock confirmed that in the UK 'interception might be undertaken only with the Secretary of State's authority given by a warrant of his own hand'.[147] Secret surveillance was justified by forwarding of threats and opportunities. Spying maintains power relative to competitors. Hence, in *Privacy International v Secretary of State*[148] the Court of Appeal dismissed an appeal by numerous NGOs claiming that the government's 'Guidance on the Use of Agents who Participate in Criminality' was unlawful. In its early responses, European Court jurisprudence rejected hypothetical claims regarding damages that are yet to materialise, on grounds that the data subject is unsure and could not substantiate his claims. Since the claimant could not show that he himself had been a direct or indirect victim of a violation of the European Convention on Human Rights, a public interest litigation basis was rejected.[149] However, with the emergence of big data decisions, claimants with hypothetical grievances now attain recognition and remedies. For example, in *Klass v Germany*, there existed a legislative framework governing the use of covert intelligence, potentially affecting all users of postal and telecommunications services. Similarly, in *Hilton v UK*,[150] the Court held that there had to be at least reasonable likelihood that

143 MK Addo 'Political self-determination within the context of the African Charter on Human and Peoples' Rights (1988) 32 *Journal of African Law* 182-193.
144 Nwauche (n 37) 84.
145 Bermingham (n 97) 269-270.
146 Abdulrauf (n 38) 120-121.
147 Delany and Others (n 55) 46.
148 [2021] EWCA Civ 330; 2 WLR 1333.
149 Van der Sloot (n 2) 417.
150 [1978] 2 EHRR 214.

the Security Service has compiled and continues to retain personal information regarding the claimants.[151] Nowadays it is accepted, in Europe at any rate, that the mere existence of an intrusive law at domestic level, may lead to interference with the right to privacy contravening the European Convention.[152] Notwithstanding the fact that some claimants were yet to be subjected to surveillance measures, the courts have struck down surveillance laws and practices to alleviate a chilling effect. Clearly, the Kenyan Court of Appeal decision in the *Mobile Telephones* case is irreconcilable not only with EU, but also global, data protection laws.

The UN's draft Legal Instrument on Government-led Surveillance and Privacy (LIGSP) crystallised from meetings and correspondence between the MAPPING project and several stakeholder categories designing the development and utilisation of digital technologies. They comprise leading global technology companies, experts experienced in working within civil society, law enforcers, intelligence services, academicians and diverse multi-stakeholder community members shaping the internet and the transition to the digital age.[153] Emergent consensus is that human rights should be considered as a single entity, encompassing the rights of people to develop their lives and personalities in a similar manner to the rights of crime victims and of individuals to inhabit safe and secure surroundings.[154] In the digital age, it emphasises the promotion and protection of human rights.[155] It rejects bulk interception carried out by police. However, the digital technologies used to conduct surveillance are becoming increasingly identical. Sometimes multiple state agencies use them or they are provided by third-party vendors. Thus, LIGSP aims at developing provisions that fully defend, respect and preserve human rights not limited to public safety, fair trial rights and victim's rights, but also privacy and personality rights. Mimicking the EU's stance, LIGSP thus propounds that all human rights stem from human dignity. It has become highly important to construct confidence and trust in the internet, including regarding freedom of expression, privacy and other human rights. Thus, the online sphere's potential as a facilitator of development and creativity is attainable, through mutual cooperation between governments, global institutions, civil society, the private sector, the technical community and academia.[156] Focus on expressive freedoms and privacy is purposive.[157] It is essential that individual human rights are inalienable, universal and indivisible. Rather than trading-off between rights, means of their fortification and consolidation should be pursued, ultimately elevating human dignity.[158] The costs of peace are subject to sudden, intense 'fluctuations of anger, love,

151 Van der Sloot (n 2) 421.
152 *Malone v United Kingdom* [1984] ECHR 10; *PG & JH v the United Kingdom* Application 44787/98 Judgment 25 September 2001.
153 LIGSP (n 13) 2.
154 As above.
155 LIGSP (n 13) 3.
156 LIGSP (n 13) 5.
157 LIGSP (n 13) 6.
158 Art 1(9) (n 13).

contentment and aggravation'.[159] Therefore, in balancing of individual privacy with societal interests such as security, the individual right will lose. Instead, intuitionism endorses legal pluralism that accepts all,[160] including group, privacy. A DPIA may create conditions for a quantitative survey of public opinion. Politicians need to persuade the general citizenry to recognise whether to value digital surveillance to repress crime or prefer to uphold the dignity of privacy. A middle ground created, for example under sections 36 of the PTA, empowers senior police officers who reasonably suspect that terrorism-related offences have been committed to approach the High Court for an order to intercept communications. Robust safeguards precede either ordering a communications service operator to wiretap and retain specified communication, or authorising the police's entry onto premises to install interception and retention devices and to remove intercepted communications. Violating privacy contrary to court orders attracts severe penalties. PTA's section 36 is narrower than NISA's section 36. The former prescribes procedures regulating specific interception of communications to detect, deter and disrupt terrorism, thus facilitating limited surveillance conferring relatively broader privacy protections. Similarly, covert investigations targeting reasonable suspicion of other serious organised crimes are preferable to the *Mobile Telephones* precedent authorising generalised surveillance that narrows privacy, even chilling group privacy.

7 Analysis of findings

Kenya's DPA purposes to protect personal information from being shared to the detriment of data subjects. However, that Act is too narrow with respect to privacy limitations on the ground of privileging national security. Its professed consequentialism advocates a narrow approach for judicial oversight on privacy, thereby condoning surveillance. DPA exempts the processing of personal data by public authorities in the public interest or for functions which include national security or crime prevention.[161] Consequently, the power to collect or monitor is widely permissible for the personal data found in a public record or where the gathering of data from another source is essential to prevent, detect, investigate, prosecute and punish crime.[162] The Director-General of National Intelligence Service's section 36 discretion to collect personal data through surveillance is subject to obtaining special judicial warrants upon showing reasonable suspicion. However, given the emergence of big data intelligence surveillance, the state may unsuspectingly gather personal data unrelated to national security or suspicion of crime.

159 Riker (n 21) 381-382.
160 Chesterman (n 7) 244.
161 Secs 30(2)(b)(iv)-(vi) DPA (n 4).
162 Secs 28(2)(a)(i) & (f) DPA (n 4).

Because individuals cannot articulate big data's diffuse personal harm, civil society activists have lodged public interest litigation claims against the government and even corporations accused of conducting inadvertent or intentional generalised surveillance on citizens.[163] DPA's sections 28 and 30 allowing governmental intrusion into privacy are general and do not meet the constitutional necessity criterion. Invoking section 31 in *Huduma Namba*, by directing the data protection commissioner to conduct a DPIA, Judge Ngaah therefore insisted on public participation preceding roll-out. This article's contribution is that a DPIA provides an avenue for citizens' oversight enforcement of group privacy. It enforces the need to ensure that prior informed consent from data subjects as a whole is obtained as a procedural check against executive surveillance or interception of personal data. On the one hand, this retains the broad privacy approach adopted in the *Nubian Rights Forum* and *HIV* cases, requiring that surveillance should not be linked to specified persons. However, judicial oversight is limited to the initial phase and does not extend to the subsequent process, whereby personal information that is unrelated to national security may be collected while collecting the warranted data. On the other hand, notwithstanding that legislation or practice creates a reasonable likelihood that a data subject may be harmed, in the *Mobile Telephones* case the Court of Appeal was unwilling to allow for speculative claims decrying consequent chilling contingent upon generalised surveillance. Yet, given that free rider problems constrain individuals from producing public goods, civil society groups and non-legal persons are better suited than individuals to monitor generalised surveillance. Although there are constitutional and statutory bases for limiting privacy rights, there is ambiguity in big data's regulation. This article considers the applicability of data protection laws regulating big data's impact on consent by affected data-sharing subjects or victims. Based on interference with the privacy of advocate-client relationships, the LSK as a group challenged the CAK's sharing of big data. Ultimately, the Supreme Court dismissed LSK's appeal on a procedural technicality, thereby obliterating the focus on the victim requirement evinced by the 'chilling effect'.

On a group privacy concept, judicial oversight of governmental surveillance may require law enforcement agencies to ensure that the form of surveillance, although focused on a particular suspect, does not give rise to generalised surveillance. Assessment of public opinion should be preceded by a DPIA, during which affected groups may choose whether or not to 'opt in', based on objective information.[164] Individuals and groups require rights to correct data, to be forgotten and to have legal remedies. Besides the DPA, there are other statutes that broadly address some digitisation threats,[165] ranging from the NISA[166] to the

163 'A new lawsuit accuses meta of inflaming civil war in Ethiopia' *Wired* 13 December 2022, https://www.wired.com/story/meta-hate-speech-lawsuit-ethiopia/ (accessed 14 April 2023).
164 *CAK* (n 11).
165 G Mutung'u 'Kenya country report' in T Roberts and others (eds) *Surveillance law in Africa: A review of six countries* (2021) 72-101.
166 Sec 36 NISA (n 28).

Computer Misuse and Cybercrimes Act.[167] The legislature could go further by restricting the forms of technology that are used for surveillance. To prevent the government from infringing on the privacy of innocent individuals in the process of investigations of criminal suspects, there should be proper legislation to incorporate accountability, transparency and adequate oversight of surveillance systems. On the globally-dominant dignitarian model, big data collection and surveillance are viewed as unconstitutional. The burden should be placed on data processors and controllers to prove that intelligence surveillance tools, such as closed-circuit television (CCTV) cameras, ensure that third party access is highly restricted and does not violate individual or group privacy. Nowadays, given technological advancements, surveillance exceeds telecommunication channels. Yet, interception authorised under the PTA is restricted to the perpetration of terrorism-related offences or information pertaining to 'the whereabouts of the person suspected by the police officer to have committed the offence'.[168]

Data protection law confers procedural protection of substantive privacy and identity rights. The courts should strictly evaluate every application by law enforcement agencies for surveillance or search and seizures. Broad approaches to privacy demand judicial scrutiny of the surveillance purpose to ensure that such surveillance is the least restrictive in the circumstances. Curiously, in Okoiti's *Mobile Telephone* case, the Court of Appeal invoked the obsolete requirement of insisting that litigants should demonstrate individual harm by generalised surveillance. That decision was remarkably oblivious to the inherent harm that any generalised surveillance creates. However, Okoiti did not move to the Supreme Court as an aggrieved individual to reverse the Court of Appeal's narrow conception of privacy and, further, LSK's attempt to articulate grievances afflicting group privacy was technically barred. Parliament should urgently legislate to address the chilling effect that new technologies impose on both individual and group privacy. At stake is the allegedly special threat against the *inferential* privacy of groups characterised by sensitive features common to open-ended groups. Kenya's data protection laws require strengthening to adequately protect collective citizens' privacies and group identities from generalised digital surveillance.

The courts have rejected complaints that neither a privacy impact assessment nor public participation preceded the *Maisha Namba* rollout, thereby compromising citizens' biometric and biographical data.[169] In criminal procedure, first, all search operations seeking incriminating data require informed consent of suspects to volunteer information, lest investigators attract privacy breach claims protected by the right to remain silent and the freedom from trespass.[170]

167 5 of 2018.
168 Secs 36(4)(a) & (b) PTA (n 30).
169 S Kiplagat 'Court frees State to roll out Maisha Namba' *Business Daily* 23 February 2024, https://www.businessdailyafrica.com/bd/economy/court-frees-state-to-roll-out-maisha-namba-4534574 (accessed 16 March 2024).
170 Art 49(1)(b) Constitution of Kenya.

Second, even if the police do not secretly plant incriminating evidence to frame a suspect, by denying the court a chance to limit the intrusive scope of intended searches, they are deemed to harm the suspect's inherent dignity. Hence, to enshrine the presumption of innocence, 'Miranda warnings' inform arrested persons of their right against self-incrimination.[171] Where reasonable suspicion of a non-cognisable offence exists, save for special circumstances recorded by police, investigators need court warrants to authorise targeted surveillance.[172] Consequently, in *Philomena Mbete Mwilu v Director of Public Prosecutions & 3 Others*[173] Kenya's Constitutional Court excluded incriminating evidence of allegedly fraudulent bank deposits as they were discovered in Imperial Bank accounts extraneous to those that the warrants targeted. Violating privacy by unwarranted searches was detrimental to the administration of justice.

Regarding balancing, although wire taps and eavesdropping on conversations endanger privacy, nevertheless, the Constitution's article 31 privacy protection is derogable. If requesting a data subject's consent may alert them to conceal incriminating evidence or commit a crime, then *ex parte* limited warrants may be sought to intrude into an unwitting targeted suspect's private space, seeking specified data.[174] Therefore recognising the Ethics and Anti-Corruption Commission's police powers during gathering operations, including tracing assets in bank accounts, the Supreme Court exonerated EACC from issuing notice on intended targets prior to investigations.[175]

8 Conclusion

While section 36 of NISA limitedly authorises courts to permit covert investigation, monitoring or interference with the privacy of persons suspected of committing offences threatening national security, section 36 of PTA specifically authorises courts to order the interception of communications of persons reasonably suspected of terrorism-related offences. To counter potential overreaching, such as the decision handed down in the Court's blanket *Mobile Telephones* appeal, there is no reason why Parliament may not enact similar provisions to PTA to facilitate specific wiretapping while covertly investigating other transnational and organised crimes. Serious transnational crimes and the fear of these not only harm mental and physical health, but even human security and well-being which are key components of individual development.

171 Art 49(1)(a) Constitution of Kenya; see also *Miranda v Arizona* 384 US 436 (1966).
172 Secs 118 CPC (n 24) and 57 & 60 National Police Service Act 11A of 2011.
173 *Mwilu v DPP; Stanley Muluvi Kiima (Interested Party); International Commission of Jurists Kenya Chapter (Amicus Curiae)* [2019] eKLR para 349 per Omondi, Ngugi & Tuiyott JJ (as they then were); See also Constitution of Kenya (n 43) art 50(4).
174 J Wangui 'EACC has powers to secretly probe suspect's bank account, apex court rules Friday' 7 October 2022, https://nation.africa/kenya/news/eacc-has-powers-to-secretly-probe-suspect-s-bank-account-apex-court-rules-3977434 (accessed 23 January 2024).
175 *Ethics and Anti-Corruption Commission & Another v Prof Tom Ojienda* Supreme Court 30 of 2019; see also sec 180 Evidence Act (Chapter 80 Laws of Kenya).

Organised crimes also retard economic growth, distort political representation and degrade national values. In the national interest, to benefit from parallel intercept communication, legislative provisions may therefore aid senior police officers to effectively counter specific individuals suspected of piracy, poaching, counterfeiting, and of trafficking in narcotics, illegal firearms, humans or organs and even regarding corruption. This is because in their planning, preparation and perpetration, modern organised criminals invariably deploy digital technology. Africa is awash with these sophisticated devices facilitating serious vices. Consequently, it would be advantageous for criminal justice laws and policies to equip law enforcement officials with commensurate covert powers to detect the electronic and audio footprints of serious organised crimes. Catastrophic social harms accruing from organised criminal acts justify enhancing forensic tools for their detection and proof. The key limitation of the Court of Appeal's *Mobile Telephones* verdict is that it fails to require spies to demonstrate reasonable suspicion to justify obtaining of inferences from sensitive group data. It condones generalised surveillance. Conversely, requiring limited communication intercept warrants shields sensitive individuals and groups that may otherwise be inclined to 'chill' or avoid using digital spaces. Thus, promoting personal and social growth requires limiting surveillance through judiciously authorising specific intercepts to breach privacy only of those individuals who may be reasonably suspected of posing security threats. Complexly, the rise of big data compounds the challenges facing investigators of transnational organised crimes. Increasingly, sophisticated perpetrators tend to conceal themselves behind technological smokescreens in countries with which Kenya has no mutual legal assistance arrangement. While it is harder for the police to identify anonymous individuals whose communications are targeted for interceptions, they are able to infer group criminality by using big data analytics. Privacy concerns boundary management along spatial and informational aspects. In limited circumstances, where there are justifying security requirements, the judicious authorisation of targeted warrants counter-balances the harm occasioned on intercepting of digital information.

Finally, by the end of 2023, the 'Maisha Namba' database substituting the failed 'Huduma Namba' project is projected to enhance Kenya's documentation of human certificates and identity cards to enhance the management of the state's public services. The ease of identifying individuals through irises and fingerprints would dispense with the need to carry physical identity cards. However, its critics not only decry privacy erosion. They also lament possible discrimination in the recording of statistics. Beyond enacting legislation, to allay eavesdropping fears, there is a need to install firewalls, enforce regulatory compliance and punish violators. The Worldcoin company's recent processing of personal data, apparently brazenly, flouted the DPA's section 25 data protection principle compelling assurances by data processors to ensure that personal data is processed in accordance with the data subject's privacy rights. It also omitted to undertake a section 31 DPIA though public participation. A pending court case shall interpret big data analytics to determine its impact on collecting biodata

of hundreds of thousands of Kenyans for unknown purposes. Broad respect for privacy embraces the valuable role it plays in enhancing intellect, choice and personal growth. In liberal democracies, only reasonable suspicion of individual or group participation in serious crime or insecurity warrants limited state surveillance on their activities. Future research could therefore assess the security of big data technological bases, whether in private cryptosales and digital trade or outsourced by the government, including for deployment in electronic voting.