adapt

Data Practices & Protections in Kenya

Seyram Avle

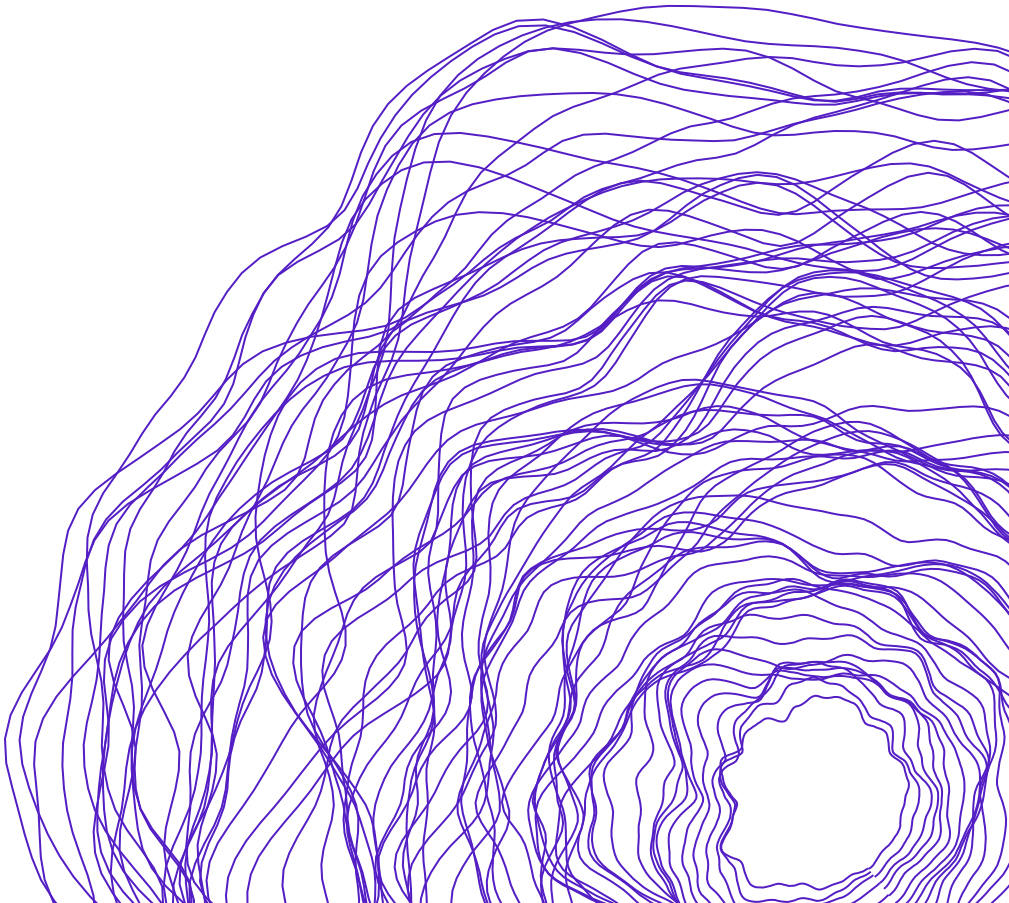

Table of Contents

List of Abbreviations

AU – African Union

CoK – Constitution of Kenya

DPA – Data Protection Act

DPC – Data Protection Commissioner

GDPR – General Data Protection Regulation

GoK – Government of Kenya

EU – European Union

NIIMS – National Integrated Identity Management System

ODPC – Office of the Data Protection Commissioner

OECD – Organization for Economic Co-operation and Development

List of Tables and Figures

Executive Summary

Since 2019, the Government of Kenya (GoK) has initiated several digitization projects that aim, among other things, to improve governance and boost the economy. As the Covid-19 pandemic wore on, new forms of data collection took hold and more surveillant practices were implemented, according to Kenyan civil society groups who have been vigilant about these changes. This report examines key aspects of the prior work done by such civil society groups, vis-à-vis the workings of the Data Protection Act (DPA) and puts them in conversation with an analysis of data practices by the state and the commercial sector. Together, these provide a landscape of how data is generated from Kenyans in their everyday encounters with the state and uses of digital technologies, and crucially, what protections are available to them.

Primarily, this report aims to provide policy makers, activists, academics, and other stakeholders with synthesized findings on how specific practices stemming from digitization in Kenya engender certain data practices and what kinds of protections citizens and consumers have. It relies primarily on a literature review on data protections and regulations in Kenya, desk research on data practices, expert, and non-expert/user interviews, as well as artifact analysis of some of the common digital devices and services in Kenya. Such a multi-faceted qualitative approach aims to provide nuance and specificity to how stakeholders might understand the gaps between data practices and protections in Kenya. Key findings include:

1) The state is a crucial data processor, sometimes in breach of its own law on data protection, a reality that fosters a lack of trust.
2) Institutions set up to implement the data protection law are underfunded, understaffed, and vulnerable to political intrusions.
3) Foreign actors have an outsized role in the extraction of Kenyan data, leading some to characterize the situation as data colonialism.
4) The technical knowledge base underpinning the implementation of data privacy, e.g., developers, have been left out of the discussion, creating a significant implementation gap.
5) There is a strong lack of awareness among the Kenyan population about the data protection law and the institutions charged with enforcing it.

Based on these findings, this report recommends a broadly more open and transparent data protection environment in Kenya. Specifically, we recommend the government work to foster public trust in how it handles citizen data by being more transparent, less data hungry, and more security conscious in how it handles any data collected, particularly in terms of encryption, domestic storage, etc. Further, we support recommendations by civil society groups to strengthen the independence of the Office of the Data Protection Commissioner by separating staff appointments from political office and providing a robust funding mechanism that will be sustainable long term. In addition, we suggest the OPDC employ a mix of “sticks and carrots” in nudging commercial actors towards greater accountability and compliance. For instance, it might include positively reinforcing and rewarding good data behavior in addition to enforcement practices such as random data audits and punishments of higher fines and penalties. Finally, the

broader challenge of global big tech and foreign extraction of Kenyan data needs to be taken seriously and urgently, with a first move being adding a more forceful (and implementable) amendment to the DPA on how foreign entities access and use Kenyan data. This might include ensuring that data is stored locally and providing a mechanism through which this can be enforced.

Information and Background

Kenya has historically served as an important connection between East African countries and the rest of the world because of its seaport along the Indian Ocean. With a population of approximately 50 million, the country has experienced various economic and political shifts since independence from the British in 1963. Most recently, "from 2015 to 2019, Kenya's economy achieved broad-based growth averaging 4.7% per year, significantly reducing poverty (which fell to an estimated 34.4% at the $1.9/day line in 2019)."[1] However, the Covid-19 pandemic disrupted trade and brought a near complete stop of tourism, a significant economic activity, in the country perhaps taking away some of these gains. Still, Kenya's government has shown resilience throughout the pandemic and has been projected to strongly rebound as travel restrictions are lifted.[2]

Kenya is also one of the most digitally connected countries in Africa.[3] Nairobi, Kenya's capital, has gained a reputation as a tech hub on the African continent, and is sometimes referred to as 'Silicon Savannah', largely due to the activities of digital technology startups that aim to provide all kinds of services to Kenyans and the rest of Africa. M-Pesa, the now classic example of mobile payments and digital activity, is integrated throughout the economy and recent government initiatives have aimed to invest more in providing Wi-Fi to entrepreneurs around the country, to drive digitization more broadly.[4] Indeed, several state reports and publications signal a desire for Kenya to be more digitally connected. Kenya's Digital Economy Blueprint and a Ministry of Information, Communication and Technology report on emerging digital technologies point to digital governance, uses of the blockchain, etc. as all essential to Kenya's economic growth and the allocation of resources.[5] Kenya is also a signatory to open data and open governance agreements and some interpretations of the Kenyan constitution argue that public participation, transparency, and accountability underscore citizens' right to access information.[6] This right to information refers both to the right to information collected and held about oneself, and to the information about the activities of the state and governing bodies whose actions affect one's life. In the many reports published on Kenya's data protection, experts link this right to information to the right to privacy which is also enshrined in the Kenyan constitution.

[1] The World Bank (2022) Kenya data.
[2] The World Bank (2022) Kenya data.
[3] Tactical tech. n.d. Kenya: Data and digital election campaigning. https://ourdataourselves.tacticaltech.org/posts/overview-kenya/ Accessed June 20, 2022.
[4] See the Ministry of ICT, Innovation, and Youth Affairs' Constituency Digital Innovation Hubs initiative here https://ict.go.ke/constituency-digital-innovation-hubs/
[5] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.
[6] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.

Privacy, according to the Constitute Project, is included in the constitutions of over 160 countries.[7] However, as Access Now points out, what this means varies widely based on "history, culture, or philosophical influences,"[8] and this variance is reflected in the disparate legal frames and practices on privacy around the world. Kenya's comprehensive data protection law derives from human and constitutional rights to privacy, some of which, it has been argued are because Kenya is a signatory to multilateral declarations and agreements such as the United Nations Declaration of Human Rights.[9] Data protection values, including those expressed in the Kenyan law, aim to help users/citizens exercise control over the uses of their data, who has access to their data, how it is used, and for how long. Without a law in place to restrict and constrain how corporations and governments use individuals' data, they will continue the practice of collecting, mining, keeping, sharing all "without telling us nothing at all."[10] **For data the protection law to be meaningful, the legal frameworks must be in tune with social expectations of citizen and consumer rights, and a broad awareness of the laws and institutions, or options, available to enforce these rights. This means understanding the embedded and emergent norms around privacy, data collection, and uses, not just from a legal or statutory perspective but from the normative viewpoint as well.**

Such a normative perspective means the everyday practices that generate data are crucial for understanding how data protection is implemented. The increased uses of digital technologies, particularly smartphones in Kenya and the rest of Africa signals a move towards more embedded digital practices in the everyday. Moreover, since 2019, the Kenyan government has been initiating several digitization projects with the aim to change governance processes and the lives of the people being governed. One participant on a data protection expert panel in Nairobi described how the GoK collected "80-90 data points in 2019 alone."[11] For instance, through the National Integrated Identity Management System (NIIMS) and Huduma Namba, the GoK aimed to create a singular way of identifying citizens by consolidating their biometric and other data into one digital identity that would also provide access to government services. With the Covid-19 pandemic came additional forms of data collection that some argue were

[7] Constitute Project https://www.constituteproject.org/constitutions?key=privacy&lang=en

[8] Access Now. 2018. Creating a data protection framework: A do's and don'ts guide for lawmakers. Lessons from the EU General Data Protection Regulation. Accessnow.org.

[9] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.

[10] Privacy International. 2017. Track, capture, kill: Inside communications surveillance and counterterrorism in Kenya. https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

[11] High level panel on 'Governing data and protecting privacy', June 30, 2022, Kenya Internet Forum. Panelists: Immaculate Kassait, *Data Commissioner, ODPC;* Sharon Holi, *Head of customer policy, Safaricom*; Irungu Houghton*, Executive Directors, Amnesty International;* Joel Karubiu, *Chief Executive Director, KENIC.* Moderator: John Walubengo. Nairobi, Kenya.

unnecessarily surveillant and fell short of standards set out in the UN's Recommendation on the Protection and Use of Health-Related Data.[12]

Civil society groups in Kenya, in general, have been vigilant about these changes, documenting and analyzing various policy instruments, digitization projects, all the while attempting to keep the GoK in check regarding data practices and protections. This report consolidates this prior work done by such civil society groups, in conjunction with desk research and artifact analysis to highlight key issues and gaps between data practices and protections available to Kenyans. More specifically, this report:

1) Maps out data practices initiated by the state and through citizen's uses of consumer products like smart phones
2) Reviews key issues of data protection as identified by civil society groups, and through both
3) Identifies areas where meaningful regulatory interventions can be made through existing and new approaches

We begin with an overview of the regulatory environment for data protection, followed by a look at some of the key issues that emerged from our review, including structural issues of governance and implementation. We focus on the state to drive home the significance of understanding government data practices while also emphasizing how commercial software and hardware function as key conduits to the datafication of the everyday.

Methods

We conducted a literature review of reports from civil organizations and examined regulatory documents from the government of Kenya on data practices and data protections in Kenya. Sources of these reports include institutions such as Amnesty International Kenya, the Kenyan ICT Network (KICTANet), the Open Institute, etc. while the desk study included reviewing online articles about the digital economy in Kenya, user practices, and other issues relevant to data protection. These were supplemented with expert and user interviews as well as insights from industry events such as the Kenya Internet Forum held in Nairobi in June 2022.[13] We combined all these with findings from artifact analysis of some of the most common smartphones (Samsung, Tecno, Infinix, itel, Xiaomi) and services (apps, M-Pesa, etc.) used in the country. The primary aim of this multifaceted qualitative approach is to provide nuanced information that can support public advocacy for data protections in Kenya that are more realistically aligned with the data practices and infrastructures being implemented 'on-the-ground' by a host of actors.

[12] Article 19 Eastern Africa, Kenya ICT Action Network, and Pollicy. 2021. Unseen Eyes, unheard stories: surveillance, data protection, and freedom of expression in Kenya and Uganda during Covid-19.
[13] Expert interviews, n=4; User interviews, n=6. Expert panelists, n=5

Data Protection in Kenya

Kenya is one of 25 African countries in the African Union (AU) with a comprehensive data protection law and an oversight mechanism.[14] Article 31 in Kenya's 2010 constitution enshrines privacy as the right to not have one's information, private affairs, or privacy of one's communications revealed. Article 35(2) of the same constitution states: "every person has the right to the correction or deletion of untrue or misleading information that affects the person."[15] Moreover, Kenyan citizens have the right to access their personal information held by both public and private entities and these entities must provide this information on request. In 2019, Kenya enacted a Data Protection Act (DPA) and through this, the Office of Data Protection Commissioner (ODPC) was established to implement and enforce the values of data protection. The use of such as Data Protection Authority, follows common practice around the globe.[16] Since its establishment, the ODPC has issued a series of guidelines including notes for electoral purposes, Huduma Namba implementation, several impact assessments, a complaints manual, etc.[17] The DPA more broadly provided guidance for the collection, storage, processing, dissemination, and transfer of personal data in Kenya and the legal recourse available for the misuse of personal data.[18]

Several international instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the African Charter on Human and People's Rights inform the DPA, as do several national policy instruments such as the GoK's Vision 2030, the National ICT policy, the Kenya Economic Blueprint for Africa, and the Kenya Digital Masterplan.[19] Some local experts' opinion was that Kenya's data protection policy bears too much similarity to the EU's GDPR, suggesting that it may not be sufficiently in tune with Kenyan needs.[20] The ODPC's independence also came up as an issue of concern in our reviews as did the state's own data practices. Still, for the most part, sources we reviewed found Kenya's data protection regulatory environment comprehensive and in step with international standards. Below are issues we found most salient across the various sources we examined.

[14] Amnesty International Kenya. November 2021. Data protection report 2021Comparative study on data protection regimes. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.
[15] Amnesty International Kenya. April 2021. Still Unaware: The state of awareness on data protection in Kenya. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.
[16] Paradigm Initiative. July 2021. Data protection authorities in Africa: A report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.
[17] https://www.odpc.go.ke/general-guidlines/
[18] See http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
[19] Bloggers Association of Kenya (BAKE). 2017. State of the internet in Kenya.
[20] One Kenyan legal expert we interviewed described it as a 'vague mimicry of European standards.'

The State as a Data Processor

Several government documents and industry reports note a desire and effort to digitize governance and the Kenyan economy.[21],[22],[23],[24] For instance, the Ministry of ICT has initiated several digitization projects including the aforementioned provision of free WIFI to support entrepreneurs through the constituency digital innovation hubs, as well as digital literacy programs in schools, a smart city initiative (Konza City), etc.[25] E-governance projects include a government website, an e-citizen platform, e-visas for foreign visitors, a Huduma Kenya portal, among others.[26] The assumption that data translates into good governance, visible in several smart city projects around the world and in projects by intergovernmental agencies such as the World Bank, is discernable in how the GoK has collected citizen data since 2019. The increased touchpoints brought on by digitization projects represent a high level of risk for the breach and abuse of data.[27]

One dominant interpretation of the Kenyan constitution in terms of data and information is that it binds citizens' right to privacy to their right to information – i.e., information about the data collected on them and data that affects their lives.[28],[29],[30],[31],[32],[33] However, we found that in practice, the two are treated as mutually

[21] Article 19 Eastern Africa, Kenya ICT Action Network, and Pollicy. 2021. Unseen Eyes, unheard stories: surveillance, data protection, and freedom of expression in Kenya and Uganda during Covid-19.

[22] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.

[23] Republic of Kenya, Emerging Digital Technologies for Kenya, Exploration and Analysis (Ministry of Information, communication and Technology, July 2019) < https://www. ict.go.ke/blockchain.pdf> accessed 18 August 2021.

[24] Republic of Kenya, Digital Economy Blueprint, Powering Kenya's transformation, <https://www.ict.go.ke/wp-content/ uploads/2019/05/Kenya-Digital-Economy-2019.pdf> Accessed June 8, 2022.

[25] see https://ict.go.ke/constituency-digital-innovation-hubs/; https://ict.go.ke/digital-literacy-programmedlp/; https://ict.go.ke/konza-city/

[26] See https://www.mygov.go.ke, https://www.ecitizen.go.ke, https://www.hudumakenya.go.ke. Huduma Kenya is described as "a Government of Kenya initiative whose aim is to turn around public service delivery by providing efficient and accessible Government services at the convenience of citizens through various integrated service delivery platforms. The Ministry of Public Service Youth and Gender Affairs is implementing the programme through the Huduma Kenya Secretariat."

[27] We discuss more of the state's data practices in section 3.2.

[28] Access Now. 2018. Creating a data protection framework: A do's and don'ts guide for lawmakers. Lessons from the EU General Data Protection Regulation. Accessnow.org.

[29] Amnesty International Kenya. November 2021. Data protection report 2021Comparative study on data protection regimes. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.

[30] Amnesty International Kenya. April 2021. Still Unaware: The state of awareness on data protection in Kenya. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.

[31] Constitution of Kenya. 2010. http://www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010 Accessed June 18, 2022.

[32] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.

[33] Restore Data Rights. 2021. A study on national and sub-national data practices in Kenya.

exclusive, with separate processes for recourse when there is a violation or breach of data. One expert described the Government of Kenya (GoK) as "quite good as withholding information from the public"[34] and stated that Freedom of Information Access (FOIA) requests often do not produce the desired outcomes because office staff so tasked are often beholden to higher placed government officials who may desire certain information to be withheld. They raised a question about how the government could effectively penalize private actors that breach the very laws that itself wasn't being held accountable to. Further, a 2021 study of national and subnational data practices by Open Initiative Kenya found that none of the five subnational governments studied used any data protection or information officers.[35] Instead, their functions were spread across a range of officers "as a peripheral duty" with few of them equipped to protect the data collected. Adding to the perception that it will be unable to keep the government in check, very little has been heard from the ODPA about how it might enforce state breaches of data privacy. This is where the independence of the commission has been up for debate, an issue we present below.

Finally, little is known about how the state stores, encrypts, and processes all the data it continually collects from citizens. Cyber security infrastructure that is impervious to hacking, is encrypted and stored locally is just as important of misuse and inappropriate sharing of data.

Independence & Sustainability of the ODPC

Studies by Amnesty International Kenya and the Open Institute Kenya found the ODPC to be independent in form but not in function.[36],[37] While the office is technically located outside of a government ministry, the position of Commissioner is a political appointment, made by the ruling executive. Other challenges center around sustainability, mainly around the issue of long-term funding and staffing (capacity) for the office. One expert we interviewed gave a table napkin calculation of the current funding available as 1 KES per Kenyan (i.e., KES 50 million for the population of ~50 million) to stress how inadequate the resources are. One report argued that without clear long-term funding, the office might have to resort to a fee-based mode of operation that will inevitably benefit the wealthy/elite in Kenya.[38] Other accounts of the ODPC express concern about the staff capacity to fulfill their mandate (specifically, adequate skillsets and expertise) with some suspicion expressed that recent hiring

[34] Interview, legal expert.

[35] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.

[36] Amnesty International Kenya. November 2021. Data protection report 2021Comparative study on data protection regimes. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.

[37] Open Institute. 2021. A study of national and (sub) national data practices in Kenya. Gaps and opportunities. Open institute Trust.

[38] Amnesty International Kenya. November 2021. Data protection report 2021Comparative study on data protection regimes. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.

efforts for the office were not transparent and favored pre-chosen candidates, an allegation the ODPC has refuted.[39] Our understanding is that Kenyan privacy and data protection experts see ODPC as an enforcer, akin to the Office of Corruption, etc., and therefore view its independence as paramount to not just the implementation of the DPA but also in obtaining and sustaining public trust.[40]

Foreign Actors and Cross-Border Processing

Despite the DP law and the establishment of the OPDP, some experts argued that there is a lack of capacity and political will to enforce cross border violations. Specifically, given the preponderance of foreign actors collecting, processing, and storing data of Kenyans, there is little in the law that empowers the ODPC to follow through on violations. One legal expert we interviewed asserted that the draft of the DPA that was circulated prior to being made law was watered down after pressure came from international actors, despite the process being meant for Kenyan citizens and Kenyan interests. By taking over the process, these actors somehow influenced the removal of stricter language on offshore processing that would have governed some of the more pernicious issues of data privacy in Kenya. [41]

Foreign actors are present both within state infrastructures and in the market. For instance, the opposition's contestation of the 2017 election results in court revealed that election data were being kept on a server in France and authorities did not readily have access to it. According to one account, "a private foreign entity, a French firm known as OT Safran Morpho, owned the information and the government struggled to get the corporation in question to make the information available on demand."[42] That same year, Huawei signed a contract with the GoK to host cloud services.[43] Earlier, in 2013, Huawei had been a crucial player for the most widely used financial platform, M-Pesa, run by Safaricom which the GoK owns 35% of. The Chinese company helped migrate the platform's then 12.8 million active users to a new one and that same mobile platform now operates in seven African countries and processes a billion transactions every

[39] Interviews. See also KICTANet's televised interview with Data Commissioner Immaculate Kassait (hosted by Grace Githaiga) here https://www.youtube.com/watch?v=6pIGqyMoyaM&t=447s

[40] High level panel on 'Governing data and protecting privacy', June 30, 2022, Kenya Internet Forum. Panelists: Immaculate Kassait, *Data Commissioner, ODPC;* Sharon Holi, *Head of customer policy, Safaricom*; Irungu Houghton, *Executive Directors, Amnesty International;* Joel Karubiu, *Chief Executive Director, KENIC.* Moderator: John Walubengo. Nairobi, Kenya.

[41] This is not yet verified at time of writing.

[42] Nyabola, Nanjala. 2019. If you are a Kenyan citizen, your private data is not safe. *The Huduma number, a new Kenyan government initiative, is yet another assault on data privacy in Kenya.* Al Jazeera. February 24, 2019. https://www.aljazeera.com/opinions/2019/2/24/if-you-are-a-kenyan-citizen-your-private-data-is-not-safe/ Accessed June 20, 2022.

[43] Mutung'u, Grace. 2018. The Influence Industry Data and Digital Election Campaigning in Kenya. Tactical Technology Collective. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

month.[44] Beijing Murong also allegedly collaborated with Huawei to introduce new features to M-Pesa. [45] As we will show in section 3, several apps and the dominant operating systems on smart phones are all from foreign actors who collect, store, and process data outside of Kenya, from the United States to Ireland. Much like in Nigeria, Ghana and elsewhere in Africa then, a significant portion of Kenyan citizen and consumer data lies in the hands of foreign corporations, both western and Chinese. The GoK has been central in these transfers, despite its own laws.

Public Participation

Public participation here is two-fold: first at the level of decision making or policy enactment process, and second, public buy-in into said policy. On the first, the Kenyan constitution requires public participation in decision making within governance processes. Experts argued that many recent initiatives that collect and store data for Kenyans, including Huduma Namba, were not subject to public input as required by the constitution. A 2020 survey conducted by Amnesty International Kenya, found that 70% of Kenyans did not hear of or participate in public events before the launch of the Huduma Namba.[46] Critics of the way Huduma Namba was put into the public domain say it contained the threat of exclusion from government services, a tactic that that we have seen in places as far flung as India with the Aadhaar system and Ghana with the Ghana Card registration. One account argued that "it is prima facie unconstitutional for a government ministry to make a "roadside declaration": to create a new legislative hurdle for gaining an important citizenship document without allowing the public time to reflect and respond."[47]

A lack of public participation is also evident when citizens do not demonstrate knowledge or familiarity with the policy instrument after it has passed. A year and a half after the DPA became law and five months after the Data Commissioner was instituted, that same Amnesty International survey found that while 54% of Kenyans are aware of their constitutional right to privacy, 67% did not know of the DPA, and only 18% knew of the

[44] Adeyemi, Daniel. 2021. M-Pesa, Opay, Telebirr, Palmpay: How Chinese tech is powering African fintech. Tech Cabal. https://techcabal.com/2021/10/07/chinas-growing-influence-is-transforming-african-tech/ Accessed July 3, 2022.

[45] See also https://carrier.huawei.com/en/success-stories/carrier-software/solutiontopic01/safaricomkenya

[46] Amnesty International Kenya. April 2021. Still Unaware: The state of awareness on data protection in Kenya. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.

[47] Nyabola, Nanjala. 2019. If you are a Kenyan citizen, your private data is not safe. *The Huduma number, a new Kenyan government initiative, is yet another assault on data privacy in Kenya.* Al Jazeera. February 24, 2019. https://www.aljazeera.com/opinions/2019/2/24/if-you-are-a-kenyan-citizen-your-private-data-is-not-safe/ Accessed June 20, 2022

establishment of the commissioner.[48] This explains why that survey also found that 53% of Kenyans did not know where to report data protection violations.

The current Data Commissioner (at time of writing) has been more public to give the office visibility and has stated that the ODPC is partnering with the Kenyan School of Government to train people on data protections. She has stressed that public awareness and legal compliance are intertwined. In addition to moving to a more centralized location in Nairobi, the OPDC has reportedly processed 422 complaints since the beginning of 2022, of which 298 have been resolved, show increasing awareness.[49] However, in some public appearances, the commissioner has also placed the burden on the public, charging that "we [Kenyans] need to start safeguarding our information… don't give information without asking why."[50] Experts we spoke to, however, argued that the lack of attention to individual privacy that the commissioner was refereeing to is largely due to general lack of understanding about how the digital economy works, not a cultural affinity towards over-sharing.

Another counter to the perspective that emphasizes individual behavior is that outside of social media, a lot of information sharing is not just by the state through its interactions with citizens but also by how it governs and instructs citizens to share data with each other. For instance, in the name of security, Kenyans must give up their identification documents to security guards to access many private and public buildings. This includes either leaving the actual document such as a driver's license, or the number of the identification document, for instance, a passport. These are often handwritten in a physical notebook or left in the guard that anyone with access can look at. This leaves one's personal information vulnerable and easily compromised.

Data Practices

In this section, we present some of the ways that various data are collected from Kenyan citizens and consumers both from industry actors and the state. Access to such information, authorized or not by the user, poses several risks that can be especially dangerous for children, marginalized groups, activists, and other vulnerable populations. It is therefore important to understand how data is collected and used, by whom, *and* what consumers understand of that process for any kind of data protection to be meaningful applied. We map out the range of commercial actors and consumer technologies that are present in the everyday, focusing on the hardware and software on smartphones largely because of the significant role they play in the increased access that Kenyans have to the internet; functioning, as it were as a gateway to the constant

[48] Amnesty International Kenya. April 2021. Still Unaware: The state of awareness on data protection in Kenya. Amnesty International Kenya and the Open Institute: Nairobi, Kenya

[49] See https://www.youtube.com/watch?v=QBzpnEtj2lQ&t=3s

[50] Ibid.

data surveillance that underlies the digital economy today. We contextualize that with what consumers know before they give consent, where consent is sought or even implied. We return to the state's actions to focus on three issues to underscore the significant role that it plays in establishing data practices and how that stands against its own laws.

Commercial Actors and Consumer Technologies

Smartphone hardware and software

Africa has the highest percentage of basic or feature phone connections (about 45%) of any region and a significant share of smartphones on the continent support 3G only.[51] This is in part due to a significant cost/affordability barrier -- the poorest 20% of individuals expect to spend more than 100% of their monthly income on an entry-level internet enabled handset and 15% of their monthly income on a data plan.[52] This cost barrier is not negligible; however, device manufacturers from the south of China have been providing low-cost smart devices to the African population in the last few years. Smart-feature phones, which do not have all the capabilities of smart phones, but still allow for a range of applications to be installed and can provide better browsing experiences than basic-feature phones, are popular with rural populations. In 2020, such phones cost about $28 USD. The most successful of these Chinese device makers, Transsion, has 3 of the top 5 brands across the continent (Tecno, Infinix, itel) and an estimated 60% of market share. Their devices span low-cost basic and smart feature phones to reasonably high-end ones that rival Apple, Samsung, and Huawei. Other phone and smart device makers have since entered the African market, with many of them operating assembly and repair centers in East (Kenya, Ethiopia) and North Africa (Egypt). The entry of smart phones, wearables, and smart devices into Africa signify a turn towards including populations that have hitherto been excluded from the digital economy and portend a shift towards increased datafication of the everyday on the continent.

In Kenya, much like the rest of the continent, Korean (Samsung) and Chinese brands (Huawei, Tecno, Infinix, Xiaomi, Oppo, etc.) dominate the market, although Apple has a presence as an aspirational brand. Except for those Apple devices, most smartphones on the market today rely on android, a system built for touch screen phones and acquired by Google in 2005. This means that majority of phones rely on Google intellectual property and are therefore enrolled into Google's data harvesting practices. Device makers often bundle their own digital products (e.g., Boomplay Music for Transsion phones) along with Google and Meta products (particularly Facebook and

[51] GSM Association (2021). The mobile economy: Sub-Saharan Africa 2021. https://www.gsma.com/mobileeconomy/sub-saharan-africa/ Accessed June 10, 2022.
[52] GSM Association (2021). The mobile economy: Sub-Saharan Africa 2021. https://www.gsma.com/mobileeconomy/sub-saharan-africa/ Accessed June 10, 2022.

WhatsApp), on all their phones. These together create user experience that requires, at a minimum, three different data policies, and in practice, several more as people download third party apps on their phones. Many products on these devices cannot be used without giving consent to access consumer files that may not be immediately related to the product or app being used. Despite a new industry standard that informs users of cookie policies and purposes for collecting data, this is considered by privacy scholars to be a meaningless exercise as consent is often coerced through the threat of non-use or obfuscated by legalese.[53]

Mobile Network/Data Providers

Telecom operators (telcos) in Kenya are some of the largest data collectors. The market is dominated by Safaricom's ~64% market share, followed by Airtel Network Kenya Ltd, a subsidiary of Airtel Africa, with a quarter of the Kenyan market.[54] One industry expert argued that Safaricom sets the tone for the industry across board, even with generating taste for specific smartphones and devices. The government's 35% stake in Safaricom presents some conflict of interest when the state regulates the sector and this arrangement has caused controversy in the past, especially with the perceived role the company plays in the state's surveillance infrastructure. In addition, Safaricom has reportedly refused to share some consumer data to small and medium enterprises (SMEs) that rely on M-Pesa, arguing that they were protecting consumer privacy.[55] However, one of the experts we interviewed argued that this only helps create a monopoly in the data value chain. Some of this data, this expert argued, was essential to business interests and could be shared in ways that do not breach consumer privacy. We spoke to at least one company that was building a platform that would enable developers, who are key stakeholders in the data infrastructure but routinely left out of the conversation, to build tailored databases that allow for varying levels of consumer data privacy and are customizable to fit regulatory dictates.

In a public forum in June 2022, the head of Safaricom's customer policy proclaimed that their data practices took cue from both the DPA and global best practices. These include communicating privacy statements on their websites and informing customers of their rights and responsibilities. Our visit to the main Safaricom website via a smartphone showed a brief notice that "this website uses cookies to ensure you get the best experience on our website. Read our cookie policy to learn more." Two options "Accept" or "Dismiss" were given, with no option to tailor the cookies, as was the global standard at the time we checked in July 2022 (see figure 1). The link to the cookie policy revealed two short notices (shorter than other policies we tested) in much more plain language that adheres better to what might be comprehensible for the lay user. At the same time,

[53] See https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html?searchResultPosition=1

[54] See https://kenyacradle.com/telecommunication-companies-in-kenya/

[55] Industry expert interview.

the option to either accept or dismiss does not give the user meaningful options. It was not clear if the cookies will be placed even if one refuses to accept or what would happen to the user experience. This brief activity gave credence to our view that 'global standards' are not necessarily a good metric in terms of respecting consumer privacy according to local law or expectations. Moreover, the ad on the main Safaricom page urged users to 'protect' their SIM cards by updating registration details. This was consistent with the language of safety, fraud prevention, etc. that governments and big industry players have used elsewhere in efforts to collect more user data. [56]

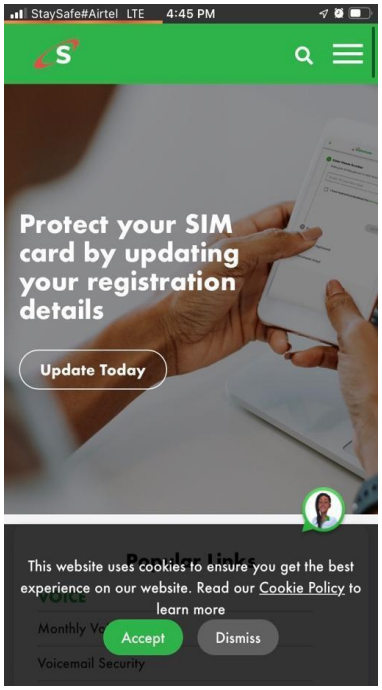

Figure 1: M-Pesa mobile website showing cookie policy

Third Party Apps

Currently, the top phone apps in the Kenyan digital space cover several different aspects of everyday life such as finances, social media, and communication (TikTok Lite, WhatsApp, FairKash, Snapchat, Facebook Lite).[57] These apps differ in the way they attract consumers and the data they collect and originate from different countries/geographies (See table 1). Fintech in Kenya has long been on the rise and has attracted venture capital from outside Kenya, largely due to how widespread M-Pesa is.[58] Within M-Pesa, a user can borrow money through a service called M-Shwari, with rates that are in part built from a history of how one saves through the platform. In some ways, saving through M-Shwari builds a credit profile that can then be used to approve or deny loans, determine

[56] See for instance, the companion report by Avle, S. and Internews, 2022. "Data Practices and Protections in Nigeria: Challenges and opportunities in the smartphone era".
[57] https://www.similarweb.com/apps/top/google/store-rank/ke/all/top-free/
[58] https://hbr.org/2021/02/kenya-is-becoming-a-global-hub-of-fintech-innovation

interest rates, etc. (see figure 2 below). FairKash, one of the most downloaded apps, provides loans for which a consumer must first register with their M-Pesa number. It functions as much of the digital banks in Nigeria, where users can borrow small amounts of money fairly quickly.

Not much is known about the developer, although there is a privacy policy on the desktop version of the Google Play store with information about what kind of data is collected, where it is stored -- "FairKash server https://hamal.fairkash.co" -- although no geographic location is given), and whether it is shared with third parties or not.[59] Crucially, the app, like many others we reviewed, collects location data, the user's personal information, financial information including transactions, all messages (including information on the sender), all contacts in address book, app activity, app performance, and device IDs.[60] The privacy policy says users have a right to request that their data be deleted but later also says they may not be able to honor this request. Related searches for FairKash Kenya in the mobile Play store returned several dozen finance apps with varying numbers of downloads, showing how much of demand/supply of access to capital there is.

App	Type	Origin
TikTok Lite	Social Media	China
WhatsApp	Chat / Social Media	USA
FairKash	Finance	?
Snapchat	Social Media	USA
Facebook Lite	Social Media	USA

Table 1: Top free android apps in Kenya[61]

Generally, banks in African countries are not consumer friendly and thus easy loans have become a lucrative business for various kinds of entities, mostly in an unregulated manner. Amnesty International Kenya estimates that about 81% of connected devices in Kenya are connected to bank and finance service as well as e-commerce.[62] An industry organization, the Digital Lenders Association (DLA) is reportedly working with the Central Bank of Kenya to become compliant with the DPA.[63] The DLA was founded in 2019 with 11 members including Tala, Alternative Circle, Stawika Capital, Zenka Finance, Okolea, Lpesa, Four Kings Investment, Kuwazo Capital and Finance Plan. Section 4.2 of

[59] Our email to the address provided in the Google Play store was returned as undeliverable. Our online search for the server returned two possible sources, China or Switzerland.

[60] See appendix A for full text of the privacy information provided by FairKash at https://app.fairkash.co/privacy.html

[61] Similar Web (June 2022)

[62] GSM Association (2021). The mobile economy: Sub-Saharan Africa 2021. https://www.gsma.com/mobileeconomy/sub-saharan-africa/ Accessed June 10, 2022.

[63] See https://www.dlak.co.ke and https://www.youtube.com/watch?v=QBzpnEtj2lQ&t=3s for more on their activities with the BoK.

their code of conduct instructs their member institutions to "a) Keep all information about the Consumer confidential, except in cases where the law allows or obliges the Institution to disclose such information to authorized institutions under the law; b) Provide security measures necessary to process and store the Consumer's personal data with full confidentiality and in accordance with applicable law; c) Ensure the transfer of Consumer's personal data only to authorized entities." [64] It is unknown at time of writing to what extent these guidelines are followed.

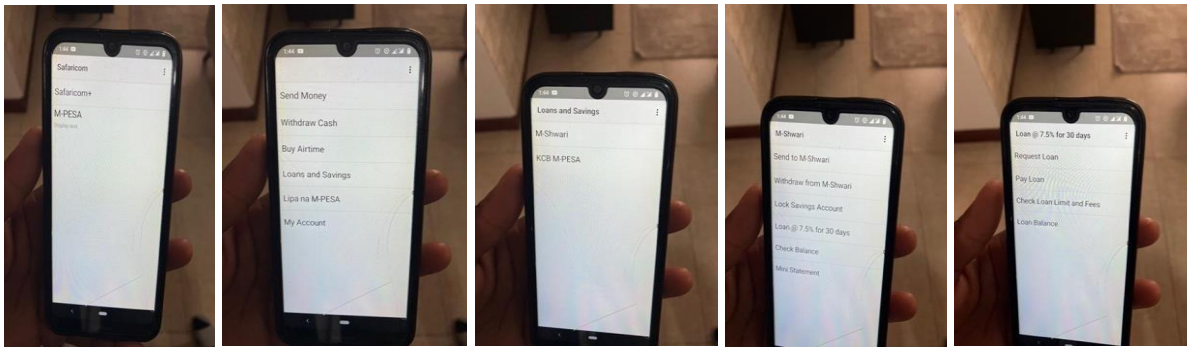

Figure 2. Screenshots of M-Pesa's platform clickthrough to M-Shwari.

State/Government Activities

As indicated in the introduction, the state has been aggressively collecting citizen data, both at the individual and county levels, ostensibly to aid security, service delivery, resource allocation, and the economy more broadly. In addition to the e-government and e-citizen portals that are in use,[65] several initiatives are in play with government-commissioned reports on everything from distributed ledger technologies to artificial intelligence (AI). Prior to the DPA, the series of "data grabs" by the state, from the census to Huduma Namba, amounted to about "80-90 data points", and Kenya saw a "proliferation of mass surveillance, including a CCTV policy" that was open to public deliberation.[66] The Covid-19 pandemic only intensified these activities. Below, we detail some of the most discussed issues that came up on the role of state activity within the data privacy and protection space.

NIIMS and Huduma Namba

One of the most ambitious and controversial projects by the state has been the issuance of Huduma Nambas through the amendment of the Registration of Persons Act (2012).[67] Section 9A of the Statute Law Act No.18 amended that Act through the establishment of

[64] See https://www.dlak.co.ke/dlak-code-of-conduct.html

[65] https://www.ecitizen.go.ke

[66] High level panel on 'Governing data and protecting privacy', June 30, 2022, Kenya Internet Forum. Panelists: Immaculate Kassait, *Data Commissioner, ODPC;* Sharon Holi, *Head of customer policy, Safaricom*; Irungu Houghton, *Executive Directors, Amnesty International;* Joel Karubiu, *Chief Executive Director, KENIC.* Moderator: John Walubengo. Nairobi, Kenya.

[67] http://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/RegistrationofPersonsActCap.%20107.pdf

the National Integrated Identity Management (NIIMS) with the intent to create a single source identity for all persons, both citizens and foreigners, living in Kenya. Huduma Namba, which loosely translates to service number, is ''a unique and permanent personal identification number randomly assigned to every resident individual at birth or upon registration/enrolment and only expires or is retired upon the death of the individual." [68]

To register, individuals provide, basic information such as name and age, their educational level, property owned and where, marital status, children, all alongside giving biometric data such as fingerprints and their photo image. The comprehensive nature of the data required to receive this digital ID created controversy, particularly as some citizens were reportedly warned that there would be consequences for not providing full details.[69] The public understanding was that this Huduma Namba would be needed to do everyday things such as registering births/deaths, applying for drivers licenses, accessing pensions, etc. The process has been challenged in court, slowing it down, with some registrants still not issued numbers at time of writing despite being fully compliant months before.

Critics of the Huduma Namba and the process involved highlight inadequate public participation, a lack of secure data protection, and the threat of exclusion from social services, among the most pernicious of issues. One study noted that other countries that have engaged in similar digital identification processes used strong security, including blockchain, cryptography, and several back up measures in the case of a breach, unlike the Kenyan state which lacked all these.[70] Other challenges include issues with user support and unclear oversight of the system.

State uses of facial recognition and artificial intelligence

In 2018, Kenya's National Police Service (NPS) announced the launch of a facial recognition system that involved the installation of CCTV cameras along highly populated areas, such as Nairobi, as well as highways and other busy roads.[71] This was ostensibly being done to upgrade Kenya's Integrated Command and Control System (ICCS). Prior to this, Kenya had also installed approximately 1,800 cameras with face and vehicle number plate recognition in highly populated areas in Nairobi and Mombasa, as well as setting up centers where all footage can be monitored in real time. This footage was accessible to most police stations in the surrounding areas that the footage was obtained from. The GoK said the goal of this project was to improve the communication between security agents, as well as enable them to be better equipped to counter

[68] See https://www.hudumanamba.go.ke/

[69] User interview

[70] *Implementing the Huduma Namba: Challenges and Prospects [change to author]*

[71] https://www.biometricupdate.com/201809/kenyan-police-launch-facial-recognition-on-urban-cctv-network#:~:text=Kenya's%20National%20Police%20Service%20

terrorist attacks that the country had been subjected to. Safaricom was sourced to develop the project with a projected cost of KES 14.9 billion (USD 169.6 million), with the expectation that they would manage the maintenance and support for the project over the course of five years.[72]

Elections

Kenyans will be going to the polls in August 2022. The ODPC reported that it had already received complaints about political parties since July 2021 about unauthorized access to citizen phone numbers and consistent spamming of political messages. These numbers were allegedly harvested from WhatsApp and M-Pesa agents[73] and other sources claimed that citizen databases are continually being sold to interested parties in the country. The Data Commissioner has been quoted as saying that she worked with the office of party registration to put out privacy notices about what data is being collected with opt outs after receiving those complaints.[74]

COVID-19 Pandemic

The COVID-19 pandemic forced people indoors and the percentage of the world's population using the internet went from 54% in 2019 to 63% in 2021.[75] Kenya's draft Guidance Note on Access to Personal Data regarding COVID-19 was issued ten months after the government's official announcement of the pandemic and the deployment of disease surveillance measures. It has been argued that the note falls short of the standards set out in the UN's Recommendation on the Protection and Use of Health-Related Data, which provides a "common international baseline for minimum standards of protection for health data."[76] It also fails to mandate the disclosure of data sharing agreements that would promote transparency and accountability and contribute to Kenya's Open Data commitments. The GoK has been further accused of disclosing personal data without consent, using telecommunications data to "track and trace" users, and deploying CCTV and Biometric tech for surveillance.[77] In effect, 50% of

[72] https://giswatch.org/en/country-report/communications-surveillance/kenya

[73] Mutung'u, Grace. 2018. The Influence Industry Data and Digital Election Campaigning in Kenya. Tactical Technology Collective. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

[74] Expert interview

[75] International Telecommunications Union (ITU) (2021). Measuring digital development. Facts and figures. ITU Development Sector. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf Accessed June 10, 2022.

[76] Bloggers Association of Kenya (BAKE). 2017. State of the internet in Kenya.

[77] Mutung'u, Grace. 2018. The Influence Industry Data and Digital Election Campaigning in Kenya. Tactical Technology Collective. https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf

Kenyans believed that data collected during the covid-19 pandemic has not been properly managed.[78]

Discussion and Conclusion

A 2021 poll by Amnesty International Kenya, roughly a year and half after the establishment of the OPDC, revealed that about half of respondents (n=1521) were aware of their constitutional right to privacy but 67% of the sample were not aware of the DPA and even fewer (18%) were aware of the ODPC.[79] However, the majority (90%) who did not know these things wanted more information after hearing about these developments. Experts interviewed for this study concurred with 53% of respondents in this poll that the lack of awareness posed the greatest barrier to Kenyans 'enjoying of data privacy'. In a joint poll conducted by the Open Institute and Amnesty International Kenya as well, 31% said they were worried about aspects of their lives being revealed online. GSM Association (2021). The mobile economy: Sub-Saharan Africa 2021. https://www.gsma.com/mobileeconomy/sub-saharan-africa/ Accessed June 10, 2022. In the policy report on implementing the Huduma Namba, it is argued that there is a broad lack of trust in the GoK to safely handle citizen data, and expert opinion across our interviews suggested that there is also a lack of political will to be more forceful on data protection given that laps in enforcement benefit the state.[80] Given the doubts about the independence of the ODPC despite being viewed as an enforcer, this presents a significant internal challenge to the fidelity and robustness of data protection in Kenya.

While civil society groups appear very much focused on establishing a working regime of privacy and data protection in Kenya, some experts in that space were of the view that their efforts are fragmented and not sufficiently coordinated to gain the kind of impact necessary. One expert believed it was important to coordinate lobbying action by writing proposals of amendments to reduce the legislative burden of law makers, and continually following up to get them passed. A few argued that the fragmentation was from a separation of stakeholders, for instance civil society groups versus industry/commercial actors like Safaricom, to come to a shared understanding of acceptable practice. One perspective from this camp that was striking was that developers who build the databases and systems that both the state and the market rely on are too often sidelined in discussions of data protections. Developers implement company and state policy in line with or in breach of law. Because of the transient nature of the software development market in Kenya, some actors could not even trace who built what and how to fix/update them into compliance following the DPA. The technical

[78] Amnesty International Kenya. November 2021. Data protection report 2021Comparative study on data protection regimes. Amnesty International Kenya and the Open Institute: Nairobi, Kenya.
[79] Amnesty International Kenya. April 2021. Still Unaware: The state of awareness on data protection in Kenya. Amnesty International Kenya and the Open Institute: Nairobi, Kenya
[80] *Implementing the Huduma Namba: Challenges and Prospects [change to author]*

knowledge underpinning data privacy and protection has been left out of the discussion, creating a significant implementation gap.

Finally, the inscrutable nature of global 'big tech' such as Google and Meta were highlighted as a vulnerability that the DPA must address. As discussed above in section 2.3, foreign extraction of Kenyan data is widespread but with no clear way of enforcing data protective behaviors. Civil society experts were of the view that the GoK and the ODPC need to challenge such actors more forcefully and without fear. Given the value of data and the fact that big tech is seeking Kenyans' and Africans' data, there is room for more assertive rulemaking as has been done elsewhere in the world.

Recommendations

What can be done to bridge these gaps and address the broader issues described above? First, we recommend amendments to the law to remove the watered-down language on foreign processing of Kenyan data. The DPA must be established as a foundational deterrent to unchecked data harvesting and exportation from offshore data processors. While borders may be seen as irrelevant to the digital economy, there are precedents elsewhere, such as in the EU and China that shows that both big and small tech can and do respond to local laws that affect their access to markets and bottom lines. The perception that individual African countries may not be significant enough belies the reality that these companies continually seek African markets and users. Kenyans' data are as important as any, are worth protecting, and governments must fulfil that fundamental responsibility of protecting their citizens.

Second, we propose that the ODPC consider employing a combination of sticks and carrots, particularly for domestic firms, in terms of rewarding/punishing DPA compliant behavior or lack thereof. For instance, rather than use the threat of reputational harm as the Data Commissioner has been heard using in public, our view (via one of the experts consulted for this report) is that perhaps building rankings and awards for the most compliant and data protective company can come to be seen as a bragging right and value point for companies. Such a 'carrot' may create a desire to do better each year. A stick to accompany that carrot might be random data audits much like the revenue service does (although the Kenyan Revenue Service itself has been accused of data breaches and surveillance) to force companies out of complacency into compliance.

During the Kenya Internet Forum in 2022, the Data Commissioner proposed the idea of alternate resolution frameworks instead of what she viewed as the default legal recourse that complainants seek. This is based on the perception that legal conflicts and processes in Kenya tend to be protracted affairs, often with few claims being actually collected even if awarded by the courts. However, arbitration or other forms of resolution frameworks presupposes that both parties agree that there is something wrong and is worth fixing. In cases where one party does not agree, this option is no longer tenable, whereas legal recourse, on the other hand, does not necessarily require

the participation of the offender at the time they are being served. We believe both options can work together, if both are seen as viable options by the parties involved.

Finally, there is the issue of the state's role in handling citizen data. Repeatedly, concerns about the lack of adequate public consultation and insufficient technical security (encryption, local storage, etc.) of citizen data highlighted the need for the GoK to be more data savvy and work to gain the trust of the people. Trust can be gained by being more transparent and responsive to actual citizens rather than foreign business interests as suggested by the DPA consultative process. This will not only strengthen the awareness of data rights but also help enforce data protection in Kenya in the long run.

Appendix A

FairKash Privacy policy collected from https://app.fairkash.co/privacy.html on July 13, 2022

PRIVACY POLICY

The permission we need you provide

To assess your eligibility and facilitate faster disbursal of your loan,we may require you to open the following permissions (you can refuse to authorize us, but this will prevent us from providing you with some business services)

SMS : We collect all your message or SMS data, To be specific, we will monitor the name of the sender, the description and the amount of transaction to perform credit risk assessment. We regularly upload your financial related information to our servers (https://hamal.fairkash.co) with a high level of protection. Your personal SMS data will not be monitored, read or shared. We will not share your collected data/all information with any third party.

CONTACTS LIST : We will collect all your phone book contacts when you give us address book permissions, including their phone contact name, phone number, contact addition date. The purpose of the collection is to establish your credit files by analyzing contact list and to increase the way to contact you. In addition, this allows you to select your references in your loan application and the information will be used for anti fraud service. All contact list will not be monitored or shared with any third party. We will upload Contact data to the FairKash server (https://hamal.fairkash.co)with high level protection.

LOCATION : We will collect your geographic location information for customer risk assessment. In some cases, you will be prompted or asked to activate the Global Positioning System (GPS) on your mobile device. We will upload location data to the Fairkash server (https://hamal.fairkash.co) with high level protection.

STORAGE : Regarding all the collected information, we will store it on the FairKash server (https://hamal.fairkash.co) with high level protection and will not be shared with any third party.

APP LIST : we will ask obtain List of your apps, and we will collect and monitor information related to your ability reported in the application, in order to identify and analyze your behavior and risk against multiple loans to assess whether the loan can be processed or not and help prevent fraud. We will upload the collected data to the FairKash server (https://hamal.fairkash.co) with high level protection.

MOBILE PHONE(DEVICE) : We may collect some of your device information, such as hardware information (including the device's operating system, Android version, IMEI number, IMSI number, MAC address, serial number, Android ID, screen size and other hardware information), and serial number to uniquely identify the device and ensure that unauthorized devices are not to act on your behalf to prevent frauds. We will upload the collected data to the FairKash server (https://hamal.fairkash.co) with high level protection.

Personal Information FairKash Collects

1、why we need to collect your information?

We collect your information to evaluate and verify your credit qualifications, to protect your account and to provide you with better customized services

2、What kind of your personal information we will collect?

1)Additional information about you to help us get to know you better, such as your gender, age, date of birth, nationality, job information and registration numbers, address, Postal code, State, Province, National ID;

2)Financial information needed to process loans and payments, such as Mobile money statements, M-pesa number.

3)We will collect data from your device for our credit scoring system. This includes information relating to your device, such as device maker and model, operating system, installed software applications, and the unique user identifier.

4)We also collect your email and Contacts List and information related to device activity such as SMS logs and GPS location information.

3、How do we protect your personal information.

Your information will be encrypted by us and uploaded to our own server (https://hamal.fairkash.co) securely using HTTPS. We promise that we will not change your data and will not share your data with any third party. You The data will only be used by us for risk assessment analysis.

4、Your Rights

You have rights under data protection laws in relation to your personal data. These include rights to:

Request us to correct your personal data : This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request deletion of your personal data : This allows you to ask us to delete or delete personal data that we have no good reason to continue processing. You also have the right to ask us to delete or delete your personal data for which you have successfully exercised your right to object to processing (see below), where we may process your information unlawfully or where we need to delete your personal data to comply with local law. Please note, however, that due to specific legal reasons, we may not always be able to honor your removal request, and if applicable, we will notify you when you request it.

Object to processing of your personal data : where we are relying on a legitimate interest (or those of a third party). You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request the transfer of your personal data to you or a third party. We will provide you or a third party of your choice with your personal data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information for which you originally consented to our use or we use that information to contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent we may not be able to provide certain products or services to you. We will advise you if this is the case at such time when you withdraw your consent.

You can put your needs to us through our customer service email or online customer service, and we try to respond to all legitimate requests within one month. If your request is particularly complex or you have made multiple requests, it may sometimes take us more than a month. In this case, we will notify you and keep you informed.

The following Privacy Policy describes how we, FairKash collect, store, use, transfer, disclose and protect your Personal Information.

Privacy Policy

FairKash respects your right to privacy. This policy summarizes what personal information we may collect, how we may use this information, and other important topics relating to your privacy and data protection.

This Policy applies to all Internet sites and mobile applications operated by or on behalf of FairKash and includes other entities worldwide affiliated with FairKash. It also applies to personal information FairKash may otherwise collect:

(i) through our products and services;

(ii) when you interact with us by means other than a FairKash Internet Site or App, i.e. in person, by telephone, or via other means of telecommunications; and

(iii) from our employees, collectors, third party investigators, and other business partners (collectively "Business Partners"). The information obtained by FairKash will only be used for FairKash business needs relating to loans made by consumers / users of this application service, including but not limited to feasibility analysis of loan products, the need to process transactions, carry out court orders, applicable legal processes and process reports to the competent authorities.

1.FairKash Statement

To the extent required by applicable law, whenever FairKash collects personal information, FairKash will:

- Take commercially reasonable steps to ensure that your personal information is reliable for its intended use, accurate, complete, and, where necessary, kept up-to-date;
- Not use your personal information for direct marketing purposes without giving you an opportunity to "opt-out";
- Take appropriate measures, by contract or otherwise, to provide adequate protection for personal information that is disclosed to a third party or transferred to another country, including transfers within FairKash.
- This Policy constitutes as an inseparable part of FairKash Credit Agreement.

2.Information provided by you or obtained directly from your mobile device:

When you register an account in our platform, you have to provide to us certain Personal Information, including your name, National ID , date of birth, gender, education background, physical address, e-mail address, working information, marital status, emergence contact, your phone number, SIM card details, and an Account ID and/or password that you will use to access the App after registration. When you use the App, you have to provide to us such relevant information as may reasonably be required by us in order for the App to work.

3.Information collected whenever you use the App:

Device Information:

Whenever you use the App or visit our website, we may collect certain technical data about your usage, such as Internet Protocol (IP) address, information on webpages viewed, duration of each visit/session, internet Device Identity (ID) or Media Access Control address, and information about the make, model, and operating system of the device you use to access the application.

At the same time, when you use the application, you need to provide us with technical information, including the type of mobile device you use, unique device identifiers (for example, your mobile device's IMEI number, the MAC address of your mobile device's wireless network interface)), or the mobile phone number used by your mobile device), mobile network information, your mobile operating system, time zone settings. We will also collect information stored on your mobile device, including contact lists, call logs, SMS logs.

SMS Data:

We collect all your SMS data but only monitor your messages related to financial transactions. Specifically, we will monitor the sender's name, description and transaction amount for credit risk assessment. This allows us to accurately assess your credit risk. No personal SMS data is monitored, read or shared.

Contact list:

We collect all your phone book contacts including their phone contact name, phone number, date the contact was added to increase your credit profile, in addition this allows you to select your references in your loan application or easily Share our app invites to your friends.

Location:

We collect your geographic location information once a day whenever you use the app from your mobile device. In some cases, you will be prompted or asked to activate the Global Positioning System (GPS) on your mobile device so that we can provide you with a better application experience.

We strive to stop collecting your geolocation information while the app is in the background, but such information may still be collected unintentionally. You may choose to temporarily disable geolocation tracking on your mobile device at any time.

We promise that these information will be strictly encrypted and transmitted to our server (https://hamal.fairkash.co) using a secure protocol like HTTPS. We will only perform necessary analysis on your information and provide you with

personalized products. We will not change or share your information with any third party

4.Information from Business Partners and other Third Parties

- FairKash may collect personal information through our Business Partners. This information may include contact information, such as name, company name, job title, address, e-mail address, and phone number for verification and validation purposes.
- FairKash may also obtain personal information from other third-party sources, including publicly and commercially available sources. We may combine the information we receive from our Business Partners and other third-party sources with information that we collect from you, as described above.

5.FairKash Usage of Personal Information

We may use personal data for the following purposes:

To provide and maintain our Services, including monitoring the use of our Services.

Manage your account: Manage your registration as a user of the service. The personal data you provide may allow you to access different features of the service available as a registered user.

For the performance of a contract: the formulation, compliance and commitment of a purchase contract for products, goods or services you have purchased or any other contract with us through services.

To contact you: to contact you by email, phone call, text message or other equivalent form of electronic communication, such as push notifications from mobile applications regarding updates to features, products or contractual services (including security updates) or informational communications, on as necessary or reasonable.

To provide you with news, special offers and general information about other goods, services and events from us that are similar to those you have purchased or inquired about, unless you have opted out of receiving such information.

Manage Your Requests: Participate in and manage your requests to us.

For business transfers: We may use your information to evaluate or carry out a merger, divestiture, reorganization, reorganization, dissolution or other sale or transfer of some or all of our assets, whether as a going concern or as part of a bankruptcy, liquidation , or similar programs in which the personal data we hold about users of our services are assets transferred.

For other purposes: We may use your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotions and evaluating and improving our services, products, services, marketing and your experience .

We may share your personal information in the following situations:

With Service Providers: We may share your personal information with service providers to monitor and analyze the use of our services in order to contact you.

For business transfers: We may share or transfer your personal information in connection with or during negotiations of any merger, sale of company assets, financing, or the acquisition of all or part of our business to another company.

With Affiliates: We may share your information with our affiliates, in which case we will require those affiliates to comply with this Privacy Policy. Affiliates include our parent company and any other subsidiaries, joint venture partners or other companies that we control or jointly control with us.

6. Sharing of Personal Information

FairKash will not disclose your personal information except as described here:

FairKash may share your personal information with third parties we hire to perform support services for us such as but not limited to collection services among others. These third parties are required to use the personal information we share with them only to perform services on our behalf and to treat your personal information in compliance with all applicable privacy and data protection laws.

In some cases, FairKash may share your personal information with third parties who partner with us to provide products and services to our customers. If so, we will require our Business Partners to use that information in a manner consistent with this Policy, any applicable Specific Privacy Statements, and all applicable privacy and data protection laws.

FairKash may share your personal information with third parties when we have a good faith belief that disclosure is necessary:

(i) to comply with a law, regulation, court order, or other legal process;

(ii) to detect, prevent, and respond to fraud, intellectual property infringement, violation of our contracts or agreements, violation of law, or other misuse of FairKash Internet Sites, Apps, products or services;

(iii) to protect FairKash rights or property or yours or others' health, safety, welfare, rights, or property;

(iv) under similar circumstances. If such an event occurs, we will take appropriate steps to protect your personal information.

FairKash may share your personal information with third parties in connection with the reorganization, or under similar circumstances. If such an event occurs, we will take appropriate steps to protect your personal information.

Kindly note, by signing this form, you allow FairKash to share your credit information, both positive and negative with Credit Reference Bureau, and also to check your credit report for credit appraisal purposes.

FairKash may share your information with your permission or at your request.

7. Security Safeguards

Your information is highly encrypted which is completely out of readable and stored on our servers safely. Many of these databases are stored on servers located in Kenya.

FairKash maintains reasonable safeguards to protect the confidentiality, security and integrity of your personal information. Although we use security measures to help protect your personal information against unauthorized disclosure, misuse, or alteration, as is the case with all computer networks linked to the Internet, we cannot guarantee the security of information provided over the Internet and will not be responsible for breaches of security beyond our reasonable control.

FairKash shall not be held accountable or legally liable for any data breach, misuse, disclosure or unlawful sharing due to the fault of its users' failure to protect and secure their username and password or some other form of negligence.

8. Contact Us

If you have any questions about this Privacy Policy, You can contact us:

By email: support@fairkash.co

By Call: +254793263022

adapt

About the Author

Seyram Avle studies how digital technologies are made and used in the Global South, particularly as they relate to labor, identity, and futures. She currently works as Assistant Professor of Global Digital Media at the University of Massachusetts, Amherst.

Acknowledgements

Neo Nyoni (Northeastern University), Khadijah El-Usman (Paradigm Initiative, Nigeria), Grace Githaiga (KICTANet, Kenya), Meshak Masibo (KICTANet, Kenya), Internews staffers Laura Schwartz-Henderson, Benjamin Whitehead, Skylar Sallick, and the experts and users interviewed in Nigerian and Kenya.