Huduma Namba: Kenya's Transformation into an Informational State

Faith Nyaunga Nyakundi

A thesis

submitted in partial fulfillment of the

requirements for the degree of

Master of Arts in International Studies

University of Washington

2020

Committee:

Saadia M. Pekkanen

Jessica L. Beyer

Program Authorized to Offer Degree:

Jackson School of International Studies

University of Washington

Abstract

Huduma Namba: Kenya's Transformation into an Informational State

Faith Nyaunga Nyakundi

Chair of the Supervisory Committee:

Saadia M. Pekkanen

International Studies, and School of Law

In 2019, despite intense domestic public opposition, the Kenyan state established a country-wide digital registration database known as "Huduma Namba" in an effort to improve service provision, weed out fraudulent IDs, and fight against terrorism by Al-Shabaab, According to official government statements. Kenya is not alone in this data consolidation trend; several countries, including India and Turkey, have implemented centralized digital identity registries. Many scholars that have assessed the Huduma Namba implementation have highlighted the data security risks, potential exclusion of part of the population and increased surveillance. However, few have unpacked how the project empowers the state, particularly intelligence and defense apparatus, and ruling political elite. In this paper, I argue that Huduma Namba empowers these entities in the Kenyan government relative to domestic interests. This pursuit of informational power, coupled with aspects of technological determinism, inform Kenya's transition to becoming an informational state. Using theoretical frameworks on state policy choices, I examine the Huduma Namba case study between 2012 to early 2020 through government and stake-holder publications and websites, news media, and social media. This case proves useful to understanding Kenya's digital governance and transition into an informational state because it demonstrates how actors in the internal bureaucratic structure have aligned to support the move despite public opinion. Future research would expound on data privacy, security and exclusion.

Acknowledgements:

Thank you to Professors Saadia Pekkanen and Jessica Beyer for guiding me through this process, providing critical feedback that became integral in the writing of this thesis, and cheering me on. Additionally, thank you to my cohort and research groups for constructive idea exchange sessions, online and offline.

I would also like to thank my family and friends for their constant support and willingness to read and listen throughout the writing and revision process.

Table of Contents

INTRODUCTION

"Have you gotten your Huduma Namba?" My mother would inquire every time I would pick up her phone calls since the biometric registration initiative was rolled out. She would ask this jokingly, but I knew that she, just like many Kenyans, feared losing access to government services if she did not abide by the mandate to register and acquire a biometric registration number (Huduma Namba). At the time the initiative was put in place, I was studying in the US and I was equally concerned since the government said that not even Kenyans in the diaspora were exempt. Before I made a trip from Washington State to the Kenyan Embassy in Washington DC, I was curious about what this number was really about because I am skeptical of new initiatives mandated by all governments. What was supposed to be a quick search into why the government created this policy led me to studying digital governance, initiatives in the name of national security and counterterrorism, and changing my thesis and career focus to study data privacy and cybersecurity. It is in this space that I use this case of Huduma Namba to unpack the question: what accounts for the Kenyan government's move to mandate the initiative despite public domestic oppositions from Kenyan citizens and numerous experts?

In 2019, the Kenyan government rolled out registration in the new national digital database. The data would include biometric details and information on land ownership, establishments, and assets. According to the government, this was an effort to weed out fraudulent IDs and to fight against terrorism by the Al-Shabaab. Initially known as Umoja Kenya Initiative, the project is now popularly known as Huduma Namba – translated to "service number". The move by the government was swiftly opposed by members of the public and expert groups, such as Privacy International, the Center for Intellectual Property and Information Technology (CIPIT) and the Kenya Human Rights Commission (KHRC), that advocate for

privacy and against censorship by the government. Despite this opposition, the Kenyan government decided to roll out this initiative anyway.

My research seeks to answer the question: what accounts for the Kenyan government's decision to push forward with the implementation of Huduma Namba despite opposition by the public and other stakeholders? Why was the decision pushed at this specific time in Kenyan history? This inquiry falls under the social science inquiry into why states do what they do. I explore this question by analyzing state interests, both official (obtained from publicly available official government documents) and inferred (analyzed from changes to laws and regulations, and stakeholder comments related to my case study). While the government's stated reasons for the policy included increasing efficiency in service provision, counterterrorism, and fraud prevention, my analysis illustrates that it was more about increasing the powers of surveillance and censorship by the defense and intelligence departments, and the potential for manipulating elections by political leaders. Situating the Kenyan state in light of Sandra Braman's (2009) conception of an informational state, I argue that the move empowers certain entities in the Kenyan government relative to domestic interests – the move is informed by the pursuit of increased informational power that can be used for purposes such as increased surveillance and censorship, and potential manipulation of elections are central to my case. This pursuit, coupled with an aspect of technological determinism, inform Kenya's transition to becoming an informational state.

Using case study methods and textual and sentiment analysis, I explore the conversations surrounding Huduma Namba between 2012 and early 2020. The case of Huduma Namba proves useful to understanding Kenya's digital governance and transition into an informational state because it demonstrates how actors in the internal bureaucratic structure have aligned to support

the move despite public opinion. This study leaves room for further research on state-society relations, and the effects and implications of Huduma Namba to the citizen's personal security, potential alienation of sections of the population, and national security.

NIIMS, the system that ushered in Huduma Namba, was implemented under the guidance of three entities: The Steering Committee, Technical Committee, and the Secretariat.[1] Central to the implementation process is the Ministry of Interior and Coordination of National Government (State Department for Interior)[2] in conjunction with Ministry of Information, Communication and Technology (ICT).[3] The Ministry of ICT notably heads the Communications Authority of Kenya and all telecommunications agencies. These two ministries will be central to this paper's analysis, but the initiative also draws membership from others including:

> Agriculture, Livestock, Fisheries and Irrigation; Foreign Affairs; Education; Health; and State Law Office. Departments include Civil Registration; Immigration; and the National Registration Bureau. Agencies comprise of the National Transport and Safety Authority; National Hospital Insurance Fund [NHIF]; and the Kenya National Bureau of Standards [KNBS].[4]

These members make up the Secretariat, which according to the website oversees the operations of the initiative under the guidance of the Technical Committee. The Cabinet Secretary of the State Department of Interior also chairs the Steering Committee which

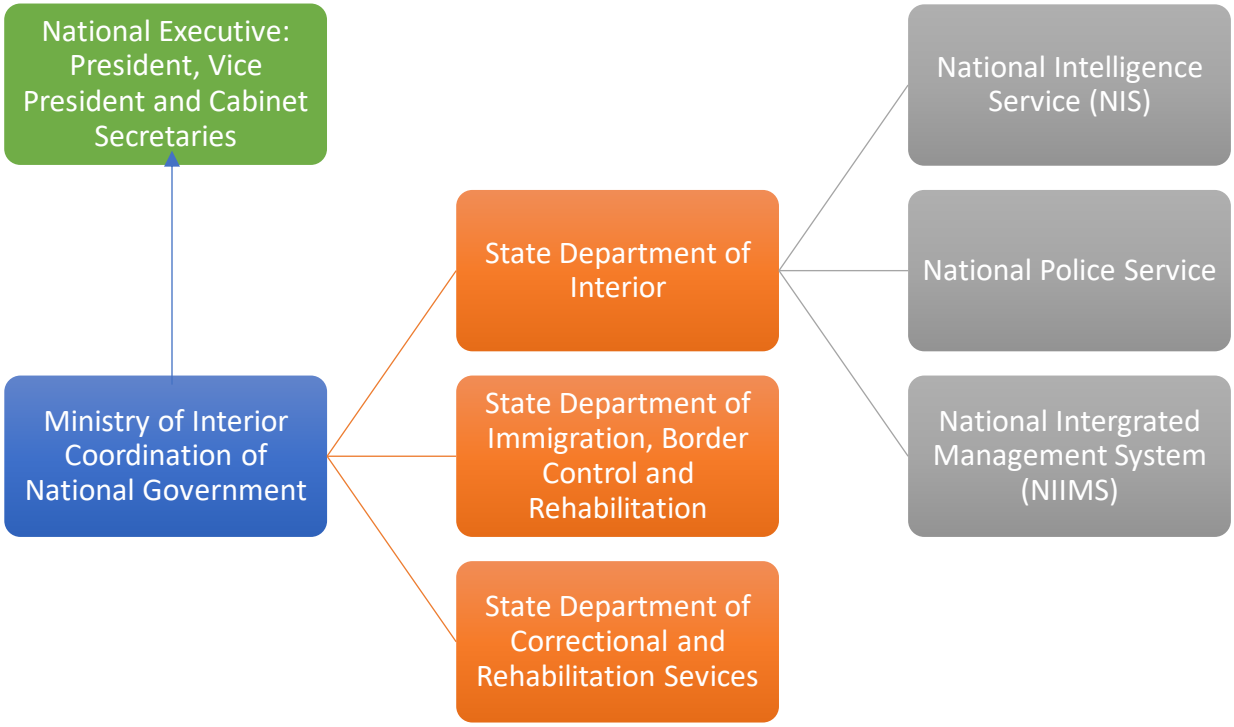
[1] Huduma Namba. *Huduma Namba Organizational Structure.* http://www.hudumanamba.go.ke/organogram/. Accessed January 2020.
[2] "Integrated Data System to Make E-government A Reality" Latest News. President of Kenya. https://www.president.go.ke/2015/03/11/integrated-data-system-to-make-e-government-a-reality/. Accessed August 10, 2020.
[3] Huduma Namba.
[4] Huduma Namba.

directs the strategy for implementation. The Steering Committee has a large task since it oversees the creation, management, and maintenance of the whole NIIMS system.

Analyzing this structure leads me to believe that the Kenyan State Department of Interior is a key actor in the implementation of Huduma Namba, so I am including an investigation of the general structure of the Ministry. It is also worth noting that in late August 2019, the Present Uhuru Kenyatta restructured the government, merging the Interior and Immigration departments via Executive Order No. 6 of 2019 to transfer additional functions to the Ministry of Interior.[5] Nested under the Ministry of Interior Coordination of National Government, the State Department of Interior and Citizens Services, "is mandated to keep the country safe and secure in accordance with the principles outlined in Article 238 (2) of the Constitution," according to its official site.[6] Also according to the site, the key agencies tasked with fulfilling that responsibility are the National Intelligence Service (NIS) and National Police Service (NPS), both of which work directly with the National Security Council which includes the defense forces and intelligence services. This paper will later demonstrate how this structure illustrates which key actors are empowered by Huduma Namba. Using Huduma Namba, a technological initiative, the Kenyan security agencies are continuously amassing informational power that can be wielded by the National Executive and the relevant cabinet secretaries. Figure 1 shows this structure, simplified to also show where the Ministry places in the hierarchical government structure.

[5] Wakaya, Jeremiah. "Kenyatta Merges Interior and Immigration Departments in Realigned Govt Structure" *Capital News*. August 29, 2019. https://www.capitalfm.co.ke/news/2019/08/kenyatta-merges-interior-and-immigration-departments-in-realigned-govt-structure/. Accessed August 11, 2020.
[6] Ministry of Interior & Coordination of National Government. *State Department for Interior and Citizen Services*. https://www.interior.go.ke/state-department-for-interior-citizen-services/.

Figure 1: Organizational Structure of Ministry of Interior (simplified)



This paper aims show to how the state is using this existing institutional structure, and through the merging of the Ministry of Interior and ICT, the leaders at the National Executive and Security Council (defense) levels are amassing information power. I will organize this argument into four sections. First, I will introduce the background to the case study, the government rhetoric around Huduma Namba, and the subsequent resistance and roadblocks to its implementation. Under the larger case study, I will highlight three use cases: one, citizen identification in provision of services; two, voter identification in elections, and three, defense and intelligence services (technology applied in war on terror). Second, I will discuss the digital/e-governance theoretical frameworks that account for the Kenyan case. Third, I will situate the Kenyan case within the discussed e-governance framework, contributing to a discussion about how Kenyan history, evidence from secondary sources, and case study

demonstrate my argument regarding Kenyan e-governance. Fourth, I will conclude with a discussion of the implications of Huduma Namba's establishment for Kenyans and further comment on Kenyans' engagement with the issue, thereby demonstrating the influence or agency of Kenyan citizens on e-governance in the country.

Using this case study, my thesis gives a macro-level view of the Kenyan state-society relations and e-governance, leaving room for further study on the agency, effects, and implications of Kenyan state digital governance for the citizenry and national security. The case of Huduma Namba proves useful to understanding Kenya's digital governance and transition into an informational state because of how actors in the internal bureaucratic structure have aligned to support the move despite public opinion. My research will contribute to the growing body of research on digital era governance, state uses of biometric and other technologies, and technological defense establishments, as well as grow the knowledge on expanding strategic digital governance in countries around the world.

Definition of Terms and concepts

According to Kenya's Center for Privacy and Information Technology (CIPIT), biometric technology collects, stores and automates pattern recognition of unique biological or behavioral characteristics of individual subjects for purposes of identification."[7] The characteristics, including fingerprints, voice, facial geometry and others, combined capture a person's biometric identity. Thales Group states that this information is then stored in a database where each person's "template" is created to be used for authentication.[8] According to Thales, the biometric

[7] Muthuri, Robert et al. Biometric Technology, elections, and Privacy. CIPIT. 2017.
[8] Thales. *Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review.* https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Accessed June 12, 2020.

authentication process involves "comparing data for the person's characteristics to that person's biometric 'template' to determine resemblance."[9] When I refer to Huduma Namba and NIIMS, I will be referring to the technology involved and how it is operationalized.

In *Biometric Recognition: Challenges and Opportunities,* the National Research Council (US) Whither Biometrics Committee add to the definition a recognition that this definition on extends to an individual person as a "body" ("human biometrics").[10] Biometric implementations are not assumed to be foolproof, since just like human-to-human recognition, they are prone to error. The authors state that automation distinguishes early biometrics from the current systems that rely on computers and human intervention.

Braman's conceptual framework of the informational state has been influential in this paper's analysis, therefore, it is important to highlight some definitions that will be used frequently in this paper. In *Change of State*, Braman sees information policy as a "manifestations of change in the very nature of governance itself."[11] Braman takes a pluralistic approach to defining information from the perspective of policy-making centers information's role as "constitutive force in society".[12] This definition that encompasses the different conceptions of information: as a commodity, as a pattern (information which reduces uncertainty), and as an agent that legally intervenes (for example, software that can act autonomously on complex decisions). Since there are different definitions, understanding information as a constitutive force

[9] Thales
[10] National Research Council (US) Whither Biometrics Committee; Pato JN, Millett LI, editors. "Biometric Recognition: Challenges and Opportunities." Washington (DC): National Academies Press (US); 2010. 1, Introduction and Fundamental Concepts. Available from: https://www.ncbi.nlm.nih.gov/books/NBK219892/
[11] Braman, Sandra. *Change of State: Information, Policy, and Power*. MIT Press. 2006. P.1.
[12] Braman, p. 21-23

captures the different conceptions as affecting information creation, processing, flows and use in different social and political settings.

Social science has always defined forms of power that shape human behaviors using different terms: instrumental (manipulating the material world via physical force), structural (manipulating the social world via rules and institutions), and symbolic (manipulating the material, social, and symbolic worlds via ideas, word, and images).[13] Braman presents a new form of power, informational which "shapes human behaviors by manipulating the informational bases of the instrumental, structural, and symbolic power."[14] Informational power, dominating the other three, can be seen in, for example, "smart weapons" which can identify a target and attack without human intervention.[15] These definitions do not assume that the other forms are obsolete, but that the new definition helps understand state interest in technological tools like Huduma Namba. This explains my use of "in transition" when defining Kenya as an informational state. The informational state is characterized by its use of policy to manipulate informational power. These are the definitions I will use throughout the paper.

ANALYTICAL FRAMEWORK

This paper tracks Huduma Namba implementation and relevant discussions between 2012 and early 2020. A deeper dive into the case, reveals that the actor interest is divided into three levels. First, there are structural or macro changes which are influenced by global trends. Kenya is fitting into a larger trend that is utilizing more technological solutions to governance choices. Huduma Namba is not the first national biometric registration system implemented by a

[13] Braman, p.25.
[14] Braman, p. 25.
[15] Braman, p. 26.

government. One of the first was India's Aadhaar which, according to Gautam Bhatia, bears some similarities to NIIMS (Huduma Namba).[16] Kenya is one among many states responding to national security crisis and challenges in service provisions. Braman's *Change of State* becomes influential throughout my paper because in addition to providing the theoretical framework for my study, she provides the backdrop to implementations of meta-technologies like Huduma Namba – the so-called war on terror. Braman, studies related policy in the USA after September 11, 2001, the advent of the Patriot Act, subsequent presumptive right of government surveillance, and the rhetoric of crisis and "national security".[17] I place Kenya in these two global trends: the use of biometric and related technologies generally, and the use of those technologies in defense and intelligence, especially during periods of perceived crises.

Second, states respond differently to perceived crisis, but according to Braman, nations are now amassing informational power in what can be perceived as technology defense. Kenya is one of the nations that responds with changes to its internal bureaucratic structure moving toward defense and intelligence establishments. As highlighted in the introduction, this study found evidence of restructuring to give more power to the ministry in charge of defense and domestic policing state departments. This ministry then partnered with the ministry leading the ICT departments and others in implementing Huduma Namba.

Third, as the theoretical framing will demonstrate that states do not act in a void; there are both internal (bottom up) and external forces, such as market or private actors. As mentioned earlier, Huduma Namba received a lot of domestic opposition from the Kenyan public and

[16] Bhatia, Gautam. "Notes From a Foreign Field: The Kenyan High Court's Judgment on the National Biometric ID System" *Indian Constitutional Law and Philosophy.* February 8, 2020. *https://indconlawphil.wordpress.com/2020/02/08/notes-from-a-foreign-field-the-kenyan-high-courts-judgment-on-the-national-biometric-id-system/.*

[17] Braman, p. 133-34

citizens, which led to its being halted by the High Court. Market or non-state actors have also influenced the adoption of Huduma Namba. These include non-Kenyan private companies such as IDEMIA and Verint whose role will be discussed later.

Although all three levels have had strong influence in this case study, this paper focuses on the second level; the internal bureaucratic (organizational) structure and the relevant actors are the focus of my analysis in this paper, leaving room for a deeper dive into the others in the future. This section provides the background of the establishment of the Huduma Namba technology and the theoretical framing to understand the case.

a) Biometrics in Kenya: Background, Opportunities and Challenges

In November 2013, the Kenyan government launched Huduma Kenya, a program that was "to turn around public service delivery by providing efficient and accessible Government services at the convenience of citizens through various integrated service delivery platforms."[18] *Huduma* is a Kiswahili word that means "service". This program was to provide a "one stop-shop" experience, and reduce bureaucracy, corruption, and inefficiency in service provision, according to the program's main site. The program began by rolling out these physical one-stop shops, Huduma Centers, in all 47 counties in Kenya to enhance accessibility.[19] In addition to that, the program included the E & M (mobile) Huduma online service, the Huduma Life, Huduma card (yet to be implemented), and Huduma Mashinani, a mobile outreach program seeking to connect with citizens at the grassroots level.[20]

[18] Huduma Kenya. https://www.hudumakenya.go.ke/huduma-kenya. Accessed November 2019.
[19] Huduma Kenya. Huduma Centers. https://www.hudumakenya.go.ke/huduma-kenya/centres. Accessed November 2019.
[20] Huduma Kenya. Huduma Mashinani. https://www.hudumakenya.go.ke/huduma-kenya/mashinani. Accessed November 2019.

In April 2014, as part of the Huduma initiative, the Kenyan government announced citizen registration in the new national digital database. This program, conducted by NIIMS, came to be popularly known as Huduma Namba. It would generate a unique number (*Huduma Namba*) with which citizens could access government services.[21] The data would include biometric details and information on land ownership, establishments, and assets. The government painted this as an effort to weed out fraudulent IDs and fight terrorism, especially considering the al-Shabaab Westgate Mall attack on September 21, 2013. Initially known as Umoja[22] Kenya, the initiative came along with large structural changes.

The Kenyan government formally initiated Huduma Namba under NIIMS (by law) through Executive Order 1 (2018) with the slogan "*Huduma Namba kwa Huduma Bora"* [service number for better service].[23] According to the order, the population database created would be "the single source of truth on a person's identity." In line with the 4th Industrial Revolution, the Kenyan government recognized that reliable data connectivity would be critical to ICT sector innovation.

In December 2012, the Ukrainian company EDAPS, completed creation of an Integrated Population Registration System (IPRS) for the Kenyan government.[24] This happened before the launch of Huduma Namba. The IPRS sought to collect preexisting data from a whole range of government agency databases: birth and death registers, the citizenship register, ID card register, aliens register, passport register and the marriage and divorce register as well as the elections

[21] Nyawira, Lyndsay. "All you need to know about the Huduma Namba." The Star. April 2, 2019. https://www.the-star.co.ke/news/2019-04-02-all-you-need-to-know-about-huduma-namba/. Accessed July 2019.
[22] "Umoja" means "togetherness" in Kiswahili.
[23] See Huduma Namba. https://www.hudumanamba.go.ke/. Accessed July 2020.
[24] Planet Biometrics. EDAPS introduces biometric portal in Kenya. January 15, 2013. https://www.planetbiometrics.com/article-details/i/1430/

register, tax register, drivers register, National Social Security Fund (NSSF) register, National Hospital Insurance Fund (NHIF) register and the Kenya National Bureau of Statistics (KNBS) register. Biometric registration was an additional layer to this pursuit.

In addition to service provision, a biometric identity system was part of Kenya's national security strategy, as stated on the site:

> The Unique Identification Number will be one of the smartest surveillance assets at major airports, entry points, and traffic checkpoints among other strategic security controls. Therefore, the police can identify possible exploits and threats for easy prioritization and subsequently enhance effective response and critical operations based on the level of the threats.[25]

The strategy document cites Kenya's need to be equipped with new means to fight various terrorist threats and organized crime which had evolved and were now using new technologies. As a justification of increased surveillance through this initiative, the document argues that any Kenyan citizen that has nothing to hide or any foreign national legally present in Kenya should have no problem with having their personal details in the new system.[26]

Huduma Namba quickly faced opposition from citizens, data security experts and human rights activists. I have been following this controversy through publications, research, and data, mainly by three organizations: Privacy International, the Center for Intellectual Property and Information Technology (CIPIT), and the Kenya High Court (through the Kenya Law site). These organizations have documented some of the controversy I will examine. There are several

[25] Huduma Admin. *Huduma Namba and Our National Security Strategy.* http://www.hudumanamba.go.ke/huduma-namba-and-our-national-security-strategy/. Accessed July 2020.
[26] Huduma admin, 2019.

reasons for pushback. First is the lack of clarity around collection, centralization and sharing. Second, the prompt way the initiative was introduced – through a Miscellaneous Act[27] which would normally involve minor law amendments meant that there was little citizen involvement in decision making.

Third, with little citizen participation, IDEMIA, a French company, was awarded the tender to provide registration gadgets (biometric kits).[28] It was unclear how IDEMIA was awarded the tender. According to Mutisya (2019), the IDEMIA had changed its name thrice in five years since it provided the "Biometric Voter Registration (BVR) kits" for the March 2013 elections as Safron Morpho and later as OT-Morpho in the 2017 elections. Mutisya (2019) reports that the company was found to be illegally conducting business in Kenya since it did not have local offices~~,~~ as required by the Kenya Companies Act (2015). After this scandal, the company was banned from conducting business in Kenya. Fourth, combined with the fact that the IPRS system was also established by a foreign company, citizens and experts questioned the lack of data protection policies to clarify how the data was collected, stored, and utilized.

Fifth, experts argue that there was possibility of exclusion of individuals from a system like NIIMS. According to Privacy International and Nubian Rights Forum, "the issues pertaining to biometric failure and lack of documentation are linked to broader social exclusion and marginalisation."[29] These organizations argued that it is risky to base access to essential services

[27] Kenya Gazette Supplement. *The Statute Law (Miscellaneous Amendments) Act, 2018*. January 4, 2019. http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMischellaneousNo18of2018.pdf.
[28] Mutisya, Musembi. The Huduma Number — Digital Identity and Inclusion in Kenya. June 7, 2019. https://pesacheck.org/the-huduma-number-digital-identity-and-inclusion-in-kenya-819ccdfd2ae0.
[29] Privacy International. *Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons*. February 24, 2020. https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

on a single system because it is a "single point of failure" (Privacy International, 2020). A single system would leave people vulnerable to technology failure, hacking, bureaucratic delays, political manipulations, and increase the government's power to exclude.[30]

Despite the controversies, biometric registration rolled out in February 2019 and by May 2019, Huduma Namba registration had collected data for 36 million citizens, according to a government claim.[31] However, the process was hit by uncertainty when the Kenyan National Assembly of Kenya voted to suspend IDEMIA from conducting business in Kenya. Additionally, there have been court rulings against the project. First, there was an April 2019 High Court ruling against making the registration exercise mandatory and collecting citizen's DNA and GPS information.[32] The Court allowed the registration to continue but demanded that the government comply with its ruling. Second, as of the completion of this paper, the latest ruling by the High Court on the matter was handed down on January 30, 2020. After petitions by privacy rights advocates, the court ruled on the amendments to the Registration of Persons Act reinforcing the earlier ruling as follows:

> The collection of DNA and GPS co-ordinates for purposes of identification is intrusive and unnecessary, and to the extent that it is not authorised and specifically anchored in empowering legislation, it is unconstitutional and a violation of Article 31 of the Constitution.[33]

[30] Privacy International, 2020.
[31] Kimani, Trizah. "36 million registered for Huduma Namba" The Star. May 24, 2019. https://www.the-star.co.ke/news/2019-05-24-36-million-registered-for-huduma-namba/.
[32] Kakah, Maureen. State barred from collecting DNA in 'Huduma Namba' Business Daily: Economy. April 1, 2019. https://www.businessdailyafrica.com/economy/State-barred-from-collecting-DNA/3946234-5052048-11jmn9v/index.html.
[33] Kenya High Court. Constitutional & Judicial Review Division: Consolidated Petitions No. 56, 58 & 59 Of 2019. January 30, 2020. http://kenyalaw.org/caselaw/cases/view/189189/.

These unique identifiers were viewed by the court as not necessary in the pursuit of governance or service provision. According to this ruling, any data collected under NIIMS cannot be utilized or processed until "appropriate and comprehensive regulatory framework on the implementation of NIIMS" that complies with the constitution, especially Article 31, is enacted (Kenya High Court, 2020). Additionally, after the Court's ruling, NIIMS registration would to be optional, have no time limits, not be a basis for denial of government or public services, and data collected would not be shared with any other entity.[34]

As was mentioned earlier, Huduma Namba is not the first national biometric registration system implemented by a government. Among the first were India's Aadhaar card[35] and Turkey's National Electronic Authentication System (eID)[36]. Just like Huduma Namba, India's and Turkey's systems are centralized systems and offer a unique identification number to individuals. In India and Turkey, the individuals are given physical cards with biometric details used for authentication. For example, in Turkey, in addition to identifying information typically found on identity cards, the Smart Card issued includes a bar code with the unique digital identity number (Turkish Republic Identity Number) and additional security features. These include antiscan and anticopy patterns, colored background printing, fine lines (guilloches) that prevent reproduction, a hologram, and miniprint, microprint, and nanoprint security features. [37] In all three countries, even with the additional security features in the Turkish system, experts raise concerns that with more citizens using these systems for identification, the risks of data

[34] Kenya High Court. Constitutional and Human Rights Division: Consolidated Petitions No. 56, 58 & 59 Of 2019. http://kenyalaw.org/caselaw/cases/view/172447/.
[35] Bhatia, Gautam. "Notes From a Foreign Field: The Kenyan High Court's Judgment on the National Biometric ID System" *Indian Constitutional Law and Philosophy.* February 8, 2020. *https://indconlawphil.wordpress.com/2020/02/08/notes-from-a-foreign-field-the-kenyan-high-courts-judgment-on-the-national-biometric-id-system/*
[36] Mutlugün, Mücahit, Adalıer, Oktay. *Turkish National Electronic Identity Card*. Research Gate. 2009.
[37] Mücahit and Oktay, p.15.

security breaches increase.[38] For instance in 2018 Adhaar was hacked, compromising the data of billions of Indians despite the government insisting that the system's security was unbreakable.[39] According to the report, the information for accessing personal data stored in the Central Repository Database was being sold on WhatsApp groups. More research on the India and Turkey cases has revealed similar approaches to implementation of these systems, and similar concerns by experts, but a thorough comparative study is outside the scope of this paper.

In summary, the Kenyan biometric registration initiative was rolled out in February 2019, Kenyan government finally initiated National Integrated Identity Management System (NIIMS) through Executive Order 1 (2018). The initiative popularly known has Huduma Namba has roots in the Huduma Kenya initiative (2012) the aim of which was to streamline service provision in the country. Huduma Namba has faced resistance from Kenyan citizens and data privacy and human rights experts since its introduction. Due to a petition to the Kenyan High Court, as of February 2020, the initiative is halted. This means all data that was collected and stored in the data collection phase cannot be used for any purposes until proper legislation and a data protection framework is implemented by the Kenyan government. As of the completion of this paper, Huduma Namba registration was an opt-in service without an opt-out process. Figure 2 illustrates the timeline to Huduma Namba implementation discussed above.

[38] Mücahit and Oktay, p.14-15.
[39] D'mello, Gwyn. "Your Worst Fears Are Realized: Aadhaar Has Been Hacked With Just A Rs 2,500 Software Patch." *IndiaTimes*, Sept 11, 2018, https://www.indiatimes.com/technology/news/your-worst-fears-are-realized-aadhaar-has-been-hacked-with-a-rs-2-500-software-patch-352859.html.

Figure 2: Background to the adoption of Huduma Namba

Background to the Adoption of Biometric Technology In Kenya

Late 2011

The Kenya government declares war on al-Shabaab, whose stronghold is in Somalia. As part of the government's counterterrorism efforts, Kenya sends troops into Somalia. Al-Shabaab increases attacks on Kenyan soil.

2011

Biometric voter registration (BVR) was made into Law by section 14 of the Elections Act. This is the first use of technology in elections. IDEMIA is contracted to provide the BVR kits.

2012

EDAPS, a Ukrainian company completed creation of an Integrated Population Registration System (IPRS) for the Kenyan government.

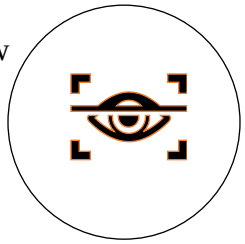
The Prevention of Terrorism Act is introduced, leading to increased surveillance.

2013

Government launches Huduma Kenya, a "one stop-shop" experience aimed at improving public service delivery by providing efficient and accessible government services through various integrated service delivery platforms.

2014

Kenyan government announces mandatory citizen registration in the new national digital database, conducted by the National Integrated Identity Management System (NIIMS). It would generate a unique number (*Huduma Namba*) to access government services.



2018

The Kenyan government initiates NIIMS through Executive Order 1 (2018) with the slogan "*Huduma Namba kwa Huduma Bora"* [service number for better service]. The database created would be "the single source of truth on a person's identity."

2019

Huduma Namba registration is rolled out in February 2019 and by May 2019, claims it has collected data on 36 million citizens.

April 2019: High Court rules against making the exercise mandatory and against collecting DNA and GPSdata.

2020

The Court rules on the amendments to the Registration of Persons Act reinforcing the earlier ruling against mandating registration and collecting DNA and GPS data.

Any data collected cannot be processed without "appropriate and comprehensive regulatory framework."

b) Theories for state choices

I seek to situate this background in theoretical framing by scholars that explore the question: why do states do what they do? In order to properly understand why the Kenyan state pushed Huduma Namba, I needed to understand Kenya's choices by explaining: first, why Huduma Namba was implemented at this specific time in history, and second, what accounts for the specific government actions (pushing Huduma Namba despite resistance). As much as this paper focuses on state choices, I do not see the state as an independent actor or the only agent unit of analysis.[40] The Huduma Namba case has shown how despite the government's ability to impose its will on society, the state is constantly being shaped and influenced by the society at large – through processes comparable to other states but also processes unique to Kenya.

There are several theories that explain state choices and how they apply to my case study. Rational choice theories, according to Joel Migdal (2001) of their insistence on collective action and the assumption that actor in government were often making choices with clear awareness of outcomes. In line with Migdal's observation, rational choice theories tended to assume that implementations of a system, Huduma Namba in this case, fail because of improper institutional structure and the lack of grounded norms and solidarity.[41] Theories along this line become especially problematic when explaining cases in Africa, as Migdal rightly points out:

> For other parts of the world, especially the newly formed countries in Asia and Africa where such normative solidarity was presumed to be absent, the focus was on the development of an ethic powerful enough to transform divergent (unharmonious) norms and institutions (often seen as traditional and inferior)… the

[40] Migdal (2001). P.8

[41] Migdal, Joel S. *State in Society: Studying How States and Societies Transform and Constitute One Another*, Cambridge University Press, 2001. P. 5

problem was wished away by assuming teleologically that modern, Western values would inevitably triumph in the end.[42]

Rational choice theory is only useful insofar as one is exploring only the states on a linear path to becoming the Western modern state. In Migdal's conception of rational choice theories, Kenya should not have been able to unify political parties and ministries in supporting the implementation of Huduma Namba. If institutions in Kenya are expected to be week, the state should not have had the capacity to roll out registration for Huduma Namba, yet it did.

Migdal's "state-in-society" approach, as a part of historical institutionalism, gives insight into the actions of the Kenyan state in relation to the domestic society. Migdal's work focuses on process which he argues "determine how societies and states create and maintain distinct ways of structuring day-to-day life" and "also ordain the ways that rules and patterns of domination and subordination are challenged and change."[43] This focus assumes that there is no single universal code or rules to determine how a society runs, or to predict how a project such as Huduma Namba will fare in a country. There are just "conflict-laden interactions of multiple sets of formal and informal guideposts for how to behave that are promoted by different groupings in society."[44]

Migdal argues that states are no different from any other formal or informal institution in this way, even though they wield significant governing power. Rules and regulations are constantly contested in unpredictable ways, so it is not just about poorly planned systems and

[42] Migdal, 2001.
[43] Migdal. P.8
[44] Migdal, p.11

policies or incompetent officials or low resources. As James Scott (1998) demonstrates, even supposedly well thought out schemes in Western nations unexpectedly fail.[45]

Migdal offers a new definition of state as a:[F]ield of power marked by the use and threat of violence and shaped by (1) the image of a coherent, controlling organization in a territory, which is a representation of the people bounded by that territory , and (2) the actual practices of its multiple parts.[46] This definition helps me situate the Kenyan state within the context of technological advancement and links this discussion to debates of governance in the digital era. The porosity of state boundaries has become especially clear with the state contracting out large projects influential to governance to large corporations, such as IDEMIA in the case of Huduma Namba.

On Digital Era Governance: Systemic explanation

While Migdal's framework proves useful in understanding the Kenyan state governance in context, there needs to be additional conceptual framework to account complex networks that make up the implementation of meta-technology projects such as Huduma Namba. Scholars of state find do not adequately explain state choices in the digital era because they downplay the role of technology, as Patrick Dunleavy et al. note in *Digital Era Governance*. Dunleavy introduces the concept of "digital era governance," arguing that his book "not only captures the previously almost uncharted government–IT industry interaction, it also shows how these relationships are central to the development of rationalization and modernization processes

[45] James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press, 1998).
[46] Migdal, p. 16

critical for the whole economic and social performance of advanced industrial states."[47] According to Dunleavy, theories, such as public administration and organization theory, often took for granted what he calls 'routinized' tasks in governance. These ignored routinized tasks include IT-support, with the result that entire IT divisions would be ignored.

Dunleavy et al. rightly predicted that many agencies would "'become their websites'—where the electronic form of the organization increasingly defines the fundamentals of what it is and does." [48] He argues that theories of **"**public administration and public management [related to Max Weber's theories of government] are among a number of factors have contributed to the under-appreciation of the contemporary salience of IT."[49] In this interdisciplinary research, I adapt Dunleavy et al.'s research theory of governance in the digital era. Even though Dunleavy's case studies (the United Kingdom, Australia, New Zealand, Japan, the Netherlands, the United States, and Canada) are different in governance compared to Kenya, Dunleavy makes compelling arguments regarding the lack of study of governance that centers the importance of IT. He argues that studies show government decision-makers engaging in,

> "strategic thinking about issues, detecting problems, setting priorities, making policy choices, carrying through implementation, managing human relations, and treating citizens equally, but all using information that is mysteriously and unproblematically at their fingertips."[50]

This lack of thorough linking of states choices to ICT and further lack of understanding intertwined nature of both development of governance alongside ICT, is very present in current

[47] Dunleavy, Patrick et al. *Digital Era Governance: IT Corporations, the State, and e-Government*. Oxford University Press, 2006. p.2
[48] Dunleavy et al., p.3.
[49] Dunleavy et al. p.4.
[50] Dunleavy et al., Chapter 2.

studies of ICT growth in Kenya and Africa at large. Most studies I have encountered continue to engage with the state as if government is always influencing IT development or vice versa.

Dunleavy et al. provide a historical path that shows the importance of information (data from paper to electronic forms) over time. The scholars also chart a path that shows the divergence of technological skills over time that led governments to outsource IT expertise to the private sector. This raises further questions regarding the relevance of the Weberian theory of a self-contained government making decisions independent of trends outside itself.

Dunleavy et al. compare states governing in the digital era to "machine bureaucracy" often associated with the private industry. They argue that like large private corporations, for example, in the "public sector the technostructure are again accountants, organization and methods, business process and operational research specialists."[51] The technostructure is part of the organizational hierarchy in machine bureaucracy. The authors argue that, today, most governing functions cannot be, "easily feasible without massive amounts of investment in information and communications technology."[52] According to Dunleavy at al., social security agencies have been central to adaptations of technology in recent times because "because their operations are central to most of governments' interactions with several key client groups."[53] , These agencies benefit from e-governments' potential to 'join-up' across several government agencies in the authors call 'whole of government' approach. As we observe in Kenya, governments "have used the rhetoric of 'joining up', a 'whole person concept', and 'one-stop

[51] Dunleavy et al., Chapter 2.
[52] Dunleavy et al.
[53] Dunleavy et al. p. 135.

shops'"[54] In the countries the authors studied, those with robust social-security programs were early adapters of IT.

They observe, for example that "Canada's HRDC [Human Resources Development Canada] was an early and successful user of IT, and its sustained buildup of internal expertise and policy of using only limited forms of outsourcing seems to have reaped some of the benefits of e-government." At the time of the study, Dunleavy et al. contrasted countries that were successfully integrating IT into social welfare programs to those that struggled with centralizing these programs. The authors argued that the sheer scale of the welfare services necessitated an adaptation of IT, which is the direction that Kenya has taken. Based on their study's prediction, Kenya would need to work to build up internal expertise for running the Huduma Namba initiative and limit outsourcing. Kenya would also need to create robust ICT policy before proceeding with implementation of any such project.

The authors generally argue for increasing the awareness in scholarship regarding the centrality of ICT in "public management theory".[55] In line with the authors' argument, the Kenyan case veers away from Weberian understandings of digital governance, recognizing the salience of ICT in a growing welfare state. This paper seeks to move away from seeing ICT as part of "routinized or technical operations" of the state in Kenya, but rather significantly influential or driving forces in policy. ICT policy in this paper, as demonstrated by the Huduma Namba case study, is an influential governance aspect that helps us understand the socio-political relations in Kenya. As discussed in the introduction, Kenya has demonstrated the importance of

[54] Dunleavy et al. p. 135.
[55] Chapter 2, 28

the ICT sector through the merger and transferring significant power to the ministries in charge of Huduma Namba.

Both these influences boosted 'institutionalist' interpretations of how government is run, which emphasized that administrative arrangements are path dependent, shaped by contingent arrangements and influenced chiefly by political and public expectations, rather than by technological or functional imperatives. This understanding leads me to the general theoretical argument of this paper: understanding Kenya as an example of an *information state*.

In C*hange of State,* Sandra Braman examines the theoretical and practical implication of the transformation or "change of the state" from the bureaucratic and welfare state to the informational state. The latter seeks to control creation, processing, flows, and use of information as an effective form of power. She examines the ways in which governments are deliberate, explicit, and consistent in their use of information policy to exercise power. She explores intellectual property rights and privacy and related policy areas that are often discussed, but not well understood. Braman introduces information policy, discussing specific contemporary problems with more abstract analysis drawn from social theory and empirical research as well as law. Braman states, "Like other complex adaptive systems, states respond to shifts in resources and in their environments."[56] These changes could be minor events or major structural changes. This becomes the basis of her argument that the adaptation of technological advancements, has seen significant structural and behavioral changes in the state. Through semi-linear processes, Braman argues that trends in information policy both manifest and trigger change in governance itself. She provides a way of understanding how information policy brings about the fundamental

[56] Braman, 29

social changes that come with the transformation to the informational state.[57] Her work is US-centric, but I utilize her generalizable definitions and adapt her theoretical framework to conceptualize Kenyan state in the era of digital governance – using Huduma Namba as the case study.

While scholars were seeing the weakening of state power, they ignored the process through which the state was changing form. Braman writes, "Because informational power has altered the materials, rules, institutions, ideas and symbols that are the means by which other forms of power are exercised, a new type of system, the informational state, has emerged".[58] She highlights three processes. First, national governments start adapting similar types of informational power as international corporations and non-state actors. Second, the state begins using private sectors for governing purposes, for example using Internet Service Providers (ISPs) to monitor the Internet in the name of national security. Third, what she considers the "networking" of the state – wherein governments become intertwined with each other and with non-state actors.[59] Where bureaucratic states heavily lean on structural power, the information state relies on information power.[60] None of the types exist in pure forms, but her typology places relative emphasis on the use of power used by each form of state, and nations are represented culturally which pays homage to state-in-society approaches.

Braman introduces the much-debated idea of technological determinism – "the idea that technologies inevitably affect society in very specific ways" which she combines with an agency-aware notion that "we are the subjects of history rather than its agents" in her analysis.

[57] Braman, p.34
[58] (Braman, p.4).
[59] Braman, p.34
[60] Braman, p.35

The latter is rather paradoxical, but her justification is that it seems like all the work being done to adapt, reinterpret, or replace specific laws or regulations is more adaptive/reactive than strategic (4-5). Nation-states are, therefore, responding to quickly evolving technologies while also utilizing them in certain ways for power – a combination of technological determinism and agency.

She argues that informational policy is thus key to understanding how this change has come about and how the nation-state exercises its power. For this reason, I investigated the policies and regulations that the Kenyan government has put forth or amended to infer how the Kenyan state is and will continue to exercise power. I have relied on interpretations for the Center for Intellectual Property and Information Policy (CIPIT), Privacy International and Kenya Law to interpret some of the legal material. This paper only scratches the surface of the theoretical discussions on the state in relation to information, but it acts as a start in adapting the discussions to explain Kenyan state choices.

c) My argument

So how do we understand the state's implementation of schemes, such as Huduma Namba? The theories discussed above ~~respond to~~ help answer my question to a certain extent. In pursuing a centralized system of identification, I ~~could~~ agree with scholars like James Scott that the state is strategically pushing a governance agenda by making its population legible (Scott, 1998), with the end goals of increasing surveillance and fighting terrorism. I also see some strategic choice in the solution the Kenyan government picked – biometric technology emerged in Kenya during the 2013 elections and the government seized the opportunity to utilize the technology and push it to other sectors beyond terrorism. As I will discuss in the evidence section, the Kenyan government had been changing rules around privacy and increasing its

surveillance capabilities before announcing the Huduma Namba initiative. However, I have also observed that rational/strategic choice theories are not sufficient in explaining why the Kenyan government is pushing this scheme now. This is specifically pointing to the declaration of the war on terror and the subsequent use of technology whose systems were installed by private non-Kenyan companies.

Historical institutionalism fills that gap by showing that state is not autonomous, but just another institution that must organize and respond to other entities within the imagined boundaries. The timing of Huduma Namba did not happen in a vacuum. When this project was first announced in 2014, the government was responding to terrorism (especially after the 2013 Westgate Mall attack by Al-Shabaab). Huduma Namba case was a strategic response to the al-Shabaab crisis.

Migdal's theoretical framework captures my understanding of the Kenyan state, but it does not fully capture the importance of the technological advancement as a phenomenon distinct from the state. This is where I merge Migdal's state-in-society argument with Dunleavy's and Nyabola's discussions of digital era governance. Huduma Namba is a case that demonstrates how digital era governance has hammered away at the public vs private divide when speaking of the state.

Biometric technology, like many new technologies, has changed the way we study the state relative to private enterprises and citizens. We cannot pursue an understanding of state choices with the assumption of state autonomy in making those choices. The Kenyan state needed to respond to crises of terrorism and critiques of service provision with improved strategies to deal with these issues, and biometric technology for identification was available and

gaining popularity. In a rational ideal-type state set up, the state would need to build capacity and skills before implementing such significant new technology. Instead we find that today states are contracting with private enterprises, such as IDEMIA, to install and run powerful governance tools. Furthermore, the data collected is not stored within country boundaries. The boundaries of governance become vague when citizen data, collected with the intention to improve governing tasks, such as service provision, crosses borders. The data is left vulnerable to multi-national private entities, such as IDEMIA, that cannot be properly "governed" or monitored, and also to security risks associated with data storage in the cloud.

Biometric technology should also influence how social scientists study the relationship between the state and the individual. As Whither Biometrics Committee states, "Unlike most other forms of recognition, biometric techniques are firmly tied to our physical bodies."[61] In a January 2020 ruling, the Kenyan High Court gave a ruling demanding to pause Huduma Namba registration, in a big victory to experts that had been petitioning the high court. In the ruling, the Court stated,

"Our view as regards the centralized storage of the biometric data of data subjects is that there will be risks of attacks or unauthorized access which exist with any storage of other personal data, but the most important risks are related to the misuse of the biometric data because this is data which are uniquely linked with individuals, which cannot be changed and are universal, and the effects of any abuse of misuse of the data are irreversible."[62]

[61] Whither Biometrics Committee, p.3
[62] Petition 56, 58 & 59 of 2019 (Consolidated). http://kenyalaw.org/caselaw/cases/view/189189/. Accessed January 2020.

The court demanded systems in place to protect citizen data since once the data was given it was out of their control. This especially stands out because it changes how we view the state as the center of governance – similar demands are not made of private companies. As institutions collect data on individuals, more people are demanding personal data protection, because unlike physical identification, systems like biometrics have significantly increased state capacity for surveillance and exclusion, despite the benefits such as service provision. Scholars of the state need to find a balance between the state and technology.

In summary, I have explored three theories to explain why the Kenyan state does what it does. Rational choice theory fit the least. Historical institutionalism (state-in-society) and systemic explanations filled the gaps left by the rational choice model. However, there was still a need for a framework to explain the use of biometric technology for governance by the state. Dunleavy introduces the idea of digital era governance as a new area for social scientists, stating that existing theories do not fully explain how the state utilizes technology, and how it affects state choices. Finally, Braman introduces the idea of the information state which shows states as entities reacting to quickly evolving technologies while also utilizing them in a certain way for power, a combination of technological determinism and agency. This is where I place Kenya. Essentially, I argue that Braman's theorization of an information state fits the Kenyan state, as evidenced by the implementation of and ensuing discussions from the Huduma Namba initiative. Table 1 summarizes the application of theoretical frameworks to evidence that will be discussed in the next section.

Rational/ Strategic Choice Theory	Historical institutionalism *State-in-society	Systemic explanation *Digital Era Governance	The information state	Evidence
X			X	Surveillance and election manipulation
X		X	X	Response to terrorism
	X	X	X	Contracting to private companies (lack of control)
			X	An aspect of technological determinism

Table 1: Summary of applied theoretical frameworks and related evidence

METHODOLOGY AND EVIDENCE

I approach this paper's main question of what accounts for Kenyan state actions in implementing Huduma Namba using mixed methods. First, I pick a case study, the Kenyan state's implementation of the National Integrated Identity Management System (NIIMS), studied between 2012 and early 2020. Second, I conduct a textual analysis of government documents, traditional media and social media debates, and stakeholder publications related to the topic of Huduma Namba. Third, I explore literature on state choices (why states do what they do) to provide this paper's theoretical framework and situate the Kenyan state in the landscape. To effectively unpack this case, I refer to literature on digital/ e-governance, biometric systems, and related technologies to understand choices and implementations for such systems on national levels.

Huduma Namba fits into the informational state model in several way. In this section, I will provide evidence to show ways in which Huduma Namba demonstrates the transformation

of the Kenyan state into an informational state also encumbered by its on historical institutionalism. At the risk of making a linear argument, the Kenyan case shows as "state in transition" to becoming one that wields informational power. We cannot fully conclude or classify Kenya in Bramanian terms, an information state, but her theoretical lens helps explain the events leading up to Huduma Namba and its implications for Kenya's governance in the digital era. There are a few contentious issues that organizations like Privacy International, KNHCR, and CIPIT have been concerned with. Some of these issues ~~are~~ were raised in the background section and I will expound on the issues of surveillance, censorship, corruption, and Kenyan electoral politics.

1. Lack of Data Protection Laws and Unclear Guidelines

Braman poses that the change of state into an informational state is characterized by a rush to amass informational power, and these schemes are implemented even in spaces lacking proper framework. This could also be by design. According to a robust report by Privacy International, *State of Privacy in Kenya*, Kenya does not have a Data Protection law or authority per se, although there are Articles built into the constitution that give some guidance.[63] As such, there is no framework to protect the biometric and alphanumeric data. Groups such as Privacy International and CIPIT have been advocating for more clear laws and a dedicated governing department. As part of this research, I explored and provide here a brief landscape of the guiding principles already in place, most of which will focus on Article 31 in the Kenyan constitution which includes stipulations that, "every person has the right to privacy, which includes the right

[63] Privacy International. *State of Privacy in Kenya*. 29 January 2019. Accessed November 2019. https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#:~:text=Once%20law%2C%20the%20Bill%20would,privacy%20of%20their%20communications%20infringed%E2%80%9D.

not to have— (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed."[64]

The Data Protection laws and amendments to those laws that I focused on are centered around 2012 as a critical year, as the Kenyan government began to focus more on this area at that time. Kenya officially declared war on al-Shabaab in October 2011 after the country faced several attacks from the group during that year.[65] After sending troops to fight them in the group's stronghold, Somalia, terrorism prevention became a big focus for the Kenyan government. Since 2012, there have been a lot of amendments to privacy guidelines where Article 31's provisions have been cut in a move to fight terrorism, as discussed in the "Background" section. These efforts were amplified by the Al Shabaab attacks in Mandera (2014), Garissa (2015)[66], and other continued incidences.[67] The recent legal developments have eroded protections against surveillance and expanded intelligence and law enforcement agencies' interception powers.

I explored some of the relevant changes and will provide a brief timeline. In 2010: Section 31 of Kenya Information and Communication Act, whose stipulations are listed about Section 12 of Kenya Information and Communication (Consumer Protection) Regulations,

[64] Kenya Law.
[65] Hussein, Farhiya. "On the Bloody Trail of Al-Shabaab Terror Attacks." Daily Nation, https://www.nation.co.ke/kenya/news/on-the-bloody-trail-of-al-shabaab-terror-attacks--842016. Accessed 1 Aug. 2020.
[66] AFP. "Al-Shabaab Militants Claim Responsibility for Garissa University Attack." *Daily Nation*, https://www.nation.co.ke/kenya/counties/garissa/al-shabaab-militants-claim-responsibility-for-garissa-university-attack-1081476. Accessed 1 Aug. 2020.
[67] Ahmed, Mohamed, Hussein, Farhiya. "20 Dead so Far as Shabaab Attacks in Kenya Escalate." Daily Nation, https://www.nation.co.ke/kenya/news/20-dead-so-far-as-shabaab-attacks-in-kenya-escalate-255288. Accessed July 1, 2020.

stipulated that no surveillance is allowed and that telecommunication providers were not allowed to disclose any information of consumers that they were serving.[68]

On August 27, 2012, The National Intelligence Service Act, 2012[69] in Article 36, "Limitation to the right to privacy," outlined, "The 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."

Article 42 stated that an officer can obtain a warrant in relation to Article 36, especially related to a "threat national security" (p.42). This language is often used in relation to terrorism in Kenya and internationally. Article 45 provided even more access members of law enforcement and intelligence obtain any information, material, record, install document and more for undefined purposes.

In 2012, the Prevention of Terrorism Act was introduced. This Act, according to Privacy International, granted more power to state law enforcement to limit freedom to privacy and from surveillance. Article 35 states, "…Subject to Article 24 of the Constitution, the rights and fundamental freedoms of a person or entity to whom this Act applies may be limited for the purposes, in the manner and to the extent set out in this section."[70]

On Feb 7, 2014, Section 13 of Kenyan Information and Communication (Registration of Subscribers of Telecommunication Services) Regulations demanded that providers grant commissioners' officers access to the information of consumers upon request. The High Court

[68] Regulation 15(1), the Kenya Information and Communications (Consumer Protection) Regulations, 2010.
[69] The Republic of Kenya. The National Intelligence Service Act, 2012. August 27, 2012. Access February 2020. https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf
[70] Privacy International, 2019.

ruled against this. Following earlier efforts to increase surveillance, in December 2014, the Security Laws (Amendment) Act 2014[71] was introduced. This included amendments to the Terrorism Prevention Act (2012), Article 69 which states: "…The right to privacy under Article 31 of the Constitution shall be limited under this section for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism."

After a push by stakeholders and the civil society, the Data Protection Bill (2015)[72] was tabled in parliament which would give effect to article 31(c) addressing several concerns on privacy protection. This was great progress for data privacy advocates, but it did not address protection of data stored in the "cloud". The cloud is defined as synchronized storage centers for digital data. It is worth noting that many cloud repository servers are based outside Kenya.

Later in 2016, a drafted Cybersecurity and Protection Bill was tabled and read in the Senate. However, this was withdrawn in December. In May 2018, Information and Communication Technology (ICT) cabinet secretary, Joe Mucheru formed a taskforce to develop a Policy and Regulatory Framework for Privacy and Data Protection in Kenya. This was after the European Union implemented the General Data Protection Regulation (GDPR) which asserted that the right to a private life and associated rights and freedoms are considered fundamental human rights.

2. Evidence of Surveillance and Censorship

In addition to changes to laws and guidelines, the Kenyan government has also demonstrated surveillance capabilities, which have been increasing with time. Among the

[71] Kenya Gazette Supplement, No. 167 (Acts No. 19). The Security Laws Amendment Act 2014.
[72] Privacy International

surveillance actors in Kenya is the National Intelligence Agency (NIS), the principal state agency where security and surveillance are concerned. It oversees both domestic and foreign intelligence in Kenya.[73] The NIS replaces the NSIS (established in 1998) which was merged with the police. Additionally, there are the National Security Council, and Kenya Police. Kenyan state actors, particularly, the General Service Unity (GSU) - paramilitary wing of the country, and the Anti-Terrorism Police Unit (ATPU) continuously surveil citizens in the name of efforts to fight terrorism.[74]

In March 2017, an investigation by Privacy International revealed that the NIS had direct access to Kenya's telecommunication networks without prior judicial authorization.[75] According to the same report, the Communications Agency and NIS could monitor individuals, the Internet and social media using technologies that enable geolocation, for example. One of the technologies highlighted was an IMSI catcher, "a phone monitoring equipment that can actively intercept communications "off-the-air" of surrounding devices".[76] The report claims that the devices capable of such interception were provided by an Israeli tech company, Verint, at least in the period 2010-2011.[77]

In a packet inspection study, CIPIT, found interception of telecommunications. CIPIT conducted a technical research project that proved the presence of a middle box on the cellular network of Safaricom Limited, the largest provider in Kenya.[78] Middle-boxes are surveillance and/or censorship software. Middle-boxes can be used in two ways: one, for legitimate functions

[73] Privacy International, 2019
[74] Privacy International. *Track, Capture Kill: Inside Communications Surveillance and Counterterrorism in Kenya*. 2017.
[75] Privacy International, 2017.
[76] Privacy International, 2017.
[77] Privacy International, 2017.
[78] CIPIT. CIPIT Reveals Evidence of Internet Tampering in the Case of Safaricom Network. Mar 23, 2017.

(like network optimization) or two, for traffic manipulation, surveillance, and aiding censorship. A situation like this called for transparency, especially with the government using the internet to monitor the 2017 elections. In this research, CIPIT conducted network measurements on Kenyan Internet Service Providers (ISPs) when they detected the middle-box on Safaricom's network. The company denied the presence of the middle-box but CIPIT noticed a lack of activity after they reached out to Safaricom for more information. Additionally, CIPIT found evidence of microtargeting in 2017 election campaigns.[79] These are instances where the government is utilizing private sectors for governing.

3. Data Privacy Invasion in the 2019 Census

In the 2019 Census, the Kenyan government unconstitutionally collected personal information from citizens, according to a CIPIT report.[80] The Kenya National Bureau of Statistics (KNBS), the office in charge of collecting census data, outlines the data to be collected: age, sex, marital status, births, deaths, migration, forms and severity of difficulties in performing of daily activities, educational attainment, labor force particulars, access and ownership of ICT equipment and services, crop farming, livestock and aquaculture, housing characteristics and ownership of assets.[81] This data is supposed to provide an overview of the population in the country and is not supposed to identify any single individual. However, according to the CIPIT report, KNBS was not clear about what data its agents could not collect. This left room for

[79] "Cambridge Analytica Had a Role in Kenya Election, Too", New York Times, 20th March 2018 https://www.nytimes. com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html
[80] Akello, Jackie, Satar, Jaaziyah. "2019 Kenya Population and Housing Census: The Data Privacy Perspective." *CIPIT Blog*. August 23, 2019. https://cipit.strathmore.edu/2019-kenya-population-and-housing-census-the-data-privacy-perspective/
[81] 2019 Kenya Population and Housing Census. https://www.knbs.or.ke/category/2019-census/

KNBS to collect information that was outside of the indicated parameters, as reported by CIPIT and other media reports. KNBS asked questions related to:

Whether individuals have registered for Huduma Namba; Identification Numbers (IDs) and names; and coordinates of an individual's place of residence – Global Positioning System (GPS) information.[82]

The information related to Huduma Namba was especially concerning because census and Huduma Namba are saliently different. The census was intended to collect only demographic information leaving the more private information for secure registration systems. "Collecting a person's identification information in this exercise may, therefore, amount to a violation of the person's right to privacy provided in Article 31" (Akello, Satar, 2019). Therefore, this is a demonstration of potential abuse of power and infringement on the data privacy rights of Kenyan citizens.

For organizations such as CIPIT, KNCHR and Privacy International, this move was worrying because it meant that the government was exploiting the loophole to scrutinize Kenyans who had not applied for Huduma Namba even though it was supposed to be optional (Akello, Satar). According the High Court rulings outlined in the Background Section, before the August 2019 census, the Kenyan government had been barred from collecting and keeping personally identifying information about its citizens. These unique identifiers were viewed by the court as not necessary in the pursuit of governance or of service provision.

All these conditions taken together show that the actions of the Kenyan government after the ruling continued to defy the court. The move to collect GPS, Huduma Namba registration

[82] Akello and Satar, 2019

status and other identifying information could be seen as bad faith by the government even if it was done by just one bureau (more evidence demonstrates that this was a trend in the government).

4. Corruption and the rhetoric of efficiency

In Kenya, it is difficult to discuss big structural changes to governance without the issue of corrupt systems being raised.[83] In addition to the issues discussed above, corruption is one of the most commonly discussed roadblocks to government provision of services and choices across Kenya. I had approached this discussion cautiously knowing the weight it carries in relation to West-centric views of African studies. As Nic Cheeseman et al. (2020) write, "Corruption—a label that can too easily stereotype Africa while downplaying similar practices in the global North—has long been a focus of everyday conversation in Kenya."[84] There are many activists and much literature that is constantly being produced in relation to this subject, and even though it is often sensationalized, it still strikes true when it comes to big projects such as the Huduma Namba initiative.

"In recent decades Kenyan news media have often mentioned the country's low rank on Transparency International's Corruption Perception Index (145th out of 176 countries in 2016). The publicity of country rankings (which of course occlude corruption's transnational dimensions) has contributed to recurrent anti-corruption promises in presidential campaigns since the 1970s."[85]

[83] Cheeseman, Nic, et al. *The Oxford Handbook of Kenyan Politics*. First ed., Oxford University Press, 2020.
[84] Cheeseman et al.
[85] Cheeseman et al.

According to activists and several other scholars, there is often disregard of public opinion, general manipulations of elections and accusations of land grabbing and mismanagement. Corruption, censorship, and surveillance were most prevalent when President Daniel Arap Moi, who ruled Kenya as a dictator for 24 years, was in office. However, these practices did not leave with him; they have continued and each candidate that runs for office promises grand reforms of some kind.[86]

The rhetoric of efficiency has also been present in the implementation of Huduma Namba – efficiency in government service provision. In Nanjala Nyabola's *Digital Democracy, Analogue Politics*, she recounts how several key agencies began moving their services to the e-citizen platform. This was by design an effort to speed up "efficient" service provision despite, "major concerns about elaborate operations to collect and store citizen data without effective data management and security policy."[87] Such structural changes, now heavily digital and reliant on informational power, are not new, and neither is the rhetoric of efficiency. This discussion of rhetoric brings the paper back to the understanding that even as scholars grapple with new ways to explain the state in the digital era, there are still situational and socio-political elements to pay attention to.

The language of reform and efficient government service provision was at the center of the last large structural change in the country, a devolution which was ushered in with the March 2013 elections. Devolution is the transfer of authority, resources, and personnel from the national to the sub-national level. As a more comprehensive form of decentralization, devolution's greatest concern is to distribute more power to the sub-national level of government, to ensure

[86] Cheeseman et al.
[87] Nyabola, p.6-7

fair distribution of resources and diffuse conflict. The idea was to distribute authority across multiple levels of government. The decision to devolve was informed by several historical triggers, one of the central ones being ethnic conflict.

Nyanjom (2011) writes, "Among the more prominent arguments for devolution – indeed, for decentralization in general – is the issue of efficiency."[88] Decentralization is expected to provide an easier flow of communication and potentially reduce the cost of transaction and service delivery. Essentially, by giving as much power, within reason, to these self-contained entities, the system becomes more efficient because the attention is focused on a smaller area. Thus, governments that decide on devolution are often triggered by the belief that the central government's inefficiency is caused by the large scope of delivery or revenue allocation.[89] It is therefore curious that the Kenyan government decided to implement a centralized system of service provision not long after the implementation of devolution.

Addressing this curiosity is, however, outside the scope of this paper. The example of devolution serves to highlight the schemes that call upon of this language of efficiency in Kenya despite many concerns that the very systems the new schemes are implementing need reviews and improvement. Treating the state as an institution, I explored the implementation process of Huduma Namba. In this section, I have provided evidence for Kenya being a state in transition to becoming an informational state through amassing information power. The lack of clear data privacy policies and guidelines, amendments to existing laws and policies to increasing government surveillance and censorship power, evidence of surveillance and privacy breaches are all provided as evidence of the informational state. Coupled with an awareness of Kenyan history,

[88] Nyanjom, Othieno. 2011. "Devolution in Kenya's New Constitution." *Constitution Working Paper no. 4.* Nairobi: Society for International Development. p.4
[89] Nyanjom, p.4.

as briefly covered in the discussion of corruption and the rhetoric of efficiency, this paper has shown the complexity of the digital transformation's influence on governance and socio-political realities in Kenya.

ASSESSMENT AND IMPLICATIONS

Drawing on major findings and analysis of the Huduma Namba cases and the technology's applied use cases, this paper provides takeaways, first, regarding the Kenyan case and future of Kenyan politics, and second, regarding what other scholars studying technology, defense applications and digital governance can learn from the Kenyan case.

First, evidence in the Kenyan case shows that the state, through the Ministry of Interior and Ministry of ICT, is amassing informational power through the centralization and near-monopolization citizen data. In line with Braman's assertion, the government is rushing to collect similar power to that of international corporations and non-state actors. As of the writing of this paper, there was no publicly available credible information providing guidance on the future design on the biometric system and who was responsible for this – the Court did not address this issue because it was a technical one and it is outside the Court's territory. There was also no clear statement regarding where and how data collected is stored and accessed. However, the biometric system, as evidenced by the state departments that have been placed in charge, is intertwined with the defense and intelligence apparatus in the country. The merging of the two ministries indicates the government's unstated intent to use information gathered through this initiative for the purpose of defense, which could have great implications for the privacy of citizens and other people living in Kenya.

Second, the government is also routinely relying on private entities for tools of governance. Some of these private entities cross state boundaries as we have seen with hiring of international companies, such as IDEMIA for important digital infrastructure. What distinguishes these contracts from those for physical infrastructure, railways for instance, is the fact that the state and these private entities become intertwined with each other, in what Braman calls the networking of the state.

Third, there are currently no clear data privacy laws and regulations for persons or a clear system in place indicating how biometric and other data is protected in Kenya. Even though there has been no credible evidence that the system has been hacked, there are risks involved in centralized digital databases as evidenced by the cases of India and Turkey.

Fourth, Kenya's rapid ICT development has offered a huge opportunity for social and economic development when combined with political action. The update of ICT sector innovations remains a challenge despite the presence of an innovative governance system. The ability of citizens to communicate through web and SMS-enabled phones, in the context of Kenya's high mobile penetration, is a critical ICT sector innovation that can ensure effective public participation and accountability during the process of determining how resources are shared. According to Data Reportal, by January 2020, there were 22.86 million internet users in Kenya, a 16% increase from 2019 bring internet penetration to 43%. 8.80 million Kenyans used social media, a 13% increase from April 2019. 98% (52.06 million) of the population is connected via mobile (not necessarily internet capable).[90] "Text messaging, email, blogging,

[90] Kemp, Simon. "Digital 2020: Kenya". *Data Reportal*. February 18, 2020. Accessed April 2020. https://datareportal.com/reports/digital-2020-kenya.

Facebook, Twitter, YouTube, Tumblr, MySpace, WhatsApp, and "citizen journalism" … have multi-generational reach.[91]

Does a strong and active society matter? Nyabola coins the term "digital democracy" to argue and provide evidence that technology is enhancing political participation (democracy) in Kenya.[92] Although this discussion is outside the scope of this paper, I want to highlight how the Kenyan citizenry uses digital tools to engage online politically to influence government decisions. I therefore only introduce the idea of digital democracy as the other side of the coin, to highlight how an agent in a public and civil society could force the government to be more thorough in implementing data protections and frameworks that protect Kenyan citizens. Cheeseman et al. highlight "how Kenyans have creatively engaged political issues outside of formal institutions since the 1980s—a period that saw political liberalization and rapid uptake of new communication technologies."[93] They explore the themes that appear in Kenya's post-1980s cultural politics of dissent, and the impact of social media and new information and communication technologies.

Kenyans use several creative means of civic engagement, for example Facebook posts, tweets, matatu inscriptions and more. Contrary to outsider observations about Kenyan and African politics, the civil society responds to and influences government actions in ways that are not often written about. The government must respond to the new platform of political engagement in civil society. According to Cheeseman et al., Kenyans are very active on Twitter

[91] Kemp, 2020.
[92] Nyabola,
[93] Cheeseman, Nic et al. "Satire, social media, and cultures of resistance." *The Oxford Handbook of Kenyan Politics*.: Oxford University Press (2020). https://www-oxfordhandbooks-com.offcampus.lib.washington.edu/view/10.1093/oxfordhb/9780198815693.001.0001/oxfordhb-9780198815693-e-18.

(#KOT) with a "global reputation for wit and winning".[94] Popular tweets include political protest organizing, satirical responses to global ignorance, traffic jam updates and more. An example was the 2015 protest against CNN "#SomeoneTellCNN". During this study, I followed #HudumaNamba intently to witness this phenomenon – the data from that observation will be left for future study.

Discussions of the agency of the people is an important aspect of understanding the state especially in relation to data privacy, surveillance, and censorship. The Whither Biometrics Committee report states, "Because biometric systems use sensed traits to recognize individuals, privacy, legal, and sociological factors are involved in all applications."[95] These complexities combined with technological shortcomings, such as systems vulnerable to hacking, and unforeseen socio-political issues often lead to extreme limitations of biometric system implementations. This paper does not aim to predict potential failures of the Huduma Namba system, but to show that even though there are numerous opportunities for the use of biometric technology, there are the Kenyan government and its peers around the world have not fully accounted or ignore these limitations.

For experts implementing meta-technological systems, and scholars looking to study to information policy related to meta-technologies, such as Huduma Namba, this paper provides general takeaways for comparative cases. First, just like in many states and other institutions implementing biometric systems, the larger system involves other technologies, environmental factors, and related policies that are "shaped by security, business, and political considerations, or idiosyncratic appeal mechanisms."[96] Even meta-technology systems that are simple,

[94] Cheeseman, Nic, et al.
[95] Whither Biometrics Committee report, p.1.
[96] National Research Council, p.1.

automated, or considered accurate are embedded in larger systems, and the two entities can mutually reinforce or negatively impact each other. As such, implementation of biometrics, and related technologies should not be studied in a vacuum, but rather understood by their intended purposes (formal and informal) and in the specific socio-political contexts. The authors' underpinning of Whither Biometrics Committee report is a systems approach

Second, one of the main trends in states amassing information power is to utilize policy to increase the surveillance capabilities of different state entities. Under the rhetoric "national security" doctrine, these policies often include the infringement in the data privacy of citizens and increase those entities' capability for surveillance and censorship – actions that can be considered a threat to democracy.[97] Braman's work provides a conceptual explanation of information in power systems controlled by the state, and how the state wields this power sometimes not in the best interest of the people. She states that informational state "increasingly knows more about individual citizens but, on the other hand, the individuals know less and less about the state"[98] The Kenyan High Court, for instance, proved that there was no reasonable explanation for the state's collection of genetic information, such as DNA. This assertion has led the domestic civil society to demand more transparency on people's privacy.

Third, courts and legal observers only commenting on laws, but not necessarily on technologies can be dangerous. As earlier discussed, when the High Court ruled on Huduma Namba, it refrained from commenting on the design on the technical systems stating that they were outside of the Court's area of expertise. The Judicial arm of the government keeps the National Executive accountable, and the design of the systems is just as important as the use of

[97] Braman, p.315.
[98] Braman, p.314.

those systems, if not more. Legal entities would need to increase the scope of their expertise to respond to the trend towards digital governance.

Robust data and personal privacy protections should be a necessity before implement a system, like Huduma Namba. Kenya could have studied the India and Turkey cases to avoid the hurdles that come with unprotected data. There has been no indication of these protections, and it was apt that Court paused the registration process until a robust framework was in place. Beyond that, there needs to be a universally agreed upon meaning of a robust data and personal privacy framework, otherwise, it leaves too much room for interpretation.

Finally, for the Huduma Namba Biometric registration system to overcome some of the glaring challenges it is facing, the Kenyan government would need to embrace a multi-stakeholder forum approach. Organizations such as CIPIT, Privacy International and others with industry knowledge are often engaging in research that provides guidelines for data protections, trust, and transparency. For example, CIPIT launched a checklist for data privacy and security in Kenyan legislations which would monitor relevant concerns as Kenya adopts more technology in its e-governance vision.[99] The Kenyan government should include more timely public participation, be transparent about the process and purpose of the data collected, and reassure Kenyans that this initiative will not exclude individuals or be used for election interference, surveillance and censorship.

[99] Wanyama, Jentrix. "CIPIT launches checklist on privacy and security in Kenyan legislations" CIPIT Blog. November 25, 2019. https://cipit.strathmore.edu/cipit-launches-checklist-on-privacy-and-security-in-kenyan-legislations-2/ Accessed July 2020.

In conclusion, this paper set out to couple an aspect of technological determinism with socio-cultural awareness in describing Kenya's digital or informational policy choices. I sought to answer the question: what accounts for the Kenyan government's push for Huduma Namba despite domestic public opposition. Applying those different theoretical frameworks to theories to my case study, I explore how the unstated or inferred interests of particular state entities, including the intelligence and defense apparatus, and the political leadership could use this data to increase surveillance and censorship, and potential manipulation of elections, are central to understanding Huduma Namba implementation. I center Braman's framework, especially the characteristics of an informational state, studying the time leading up Huduma Namba implementation (with a focus on the period between 2012 – early 2020). I argue that the implementation of Huduma Namba empowers these entities in the Kenyan government relative to domestic interests. Essentially, the move is informed by the pursuit of increased informational power in the name of counterterrorism and efficient service provision. I have provided some of the evidence for my argument. The case of Huduma Namba proves useful to understanding Kenya's digital governance and transition into an informational state because of how actors in the internal bureaucratic structure have aligned to support the move despite public opinion.

WORKS CITED

"Integrated Data System to Make E-government A Reality" Latest News. President of Kenya. https://www.president.go.ke/2015/03/11/integrated-data-system-to-make-e-government-a-reality/. Accessed August 10, 2020.

"Integrated Data System to Make E-government A Reality" Latest News. President of Kenya. https://www.president.go.ke/2015/03/11/integrated-data-system-to-make-e-government-a-reality/. Accessed August 10, 2020.

2019 Kenya Population and Housing Census. https://www.knbs.or.ke/category/2019-census/.

AFP. "Al-Shabaab Militants Claim Responsibility for Garissa University Attack." *Daily Nation,* https://www.nation.co.ke/kenya/counties/garissa/al-shabaab-militants-claim-responsibility-for-garissa-university-attack-1081476. Accessed January 8, 2020.

Ahmed, Mohamed, Hussein, Farhiya. "20 Dead so Far as Shabaab Attacks in Kenya Escalate." Daily Nation, https://www.nation.co.ke/kenya/news/20-dead-so-far-as-shabaab-attacks-in-kenya-escalate-255288. Accessed July 1, 2020.

Akello, Jackie, Satar, Jaaziyah. "2019 Kenya Population and Housing Census: The Data Privacy Perspective." *CIPIT Blog.* August 23, 2019. https://cipit.strathmore.edu/2019-kenya-population-and-housing-census-the-data-privacy-perspective/. Accessed November 20, 2019.

Beer, Jeremy De, et al. *A Framework for Assessing Technology Hubs in Africa*.

Bhatia, Gautam. "Notes From a Foreign Field: The Kenyan High Court's Judgment on the National Biometric ID System" *Indian Constitutional Law and Philosophy.* February 8, 2020. *https://indconlawphil.wordpress.com/2020/02/08/notes-from-a-foreign-field-the-*

kenyan-high-courts-judgment-on-the-national-biometric-id-system/. Accessed May 6, 2020.

Braman, Sandra. *Change of State: Information, Policy, and Power*. MIT Press, 2006.

Cheeseman, Nic, et al. *The Oxford Handbook of Kenyan Politics*. First ed., Oxford University Press, 2020.

CIPIT. CIPIT Reveals Evidence of Internet Tampering in the Case of Safaricom Network. March 23, 2017.

Dunleavy, Patrick. *Digital Era Governance: IT Corporations, the State, and e-Government*. Oxford University Press, 2006.

Huduma Admin. *Huduma Namba and Our National Security Strategy.* http://www.hudumanamba.go.ke/huduma-namba-and-our-national-security-strategy/.

Huduma Kenya. https://www.hudumakenya.go.ke/huduma-kenya. Accessed November 2019.

Huduma Kenya. Huduma Centers. https://www.hudumakenya.go.ke/huduma-kenya/centres. Accessed November 2019.

Huduma Kenya. Huduma Mashinani. https://www.hudumakenya.go.ke/huduma-kenya/mashinani. Accessed November 2019.

Huduma Namba. Huduma Namba Organizational Structure. http://www.hudumanamba.go.ke/organogram/. Accessed January 2020.

Hussein, Farhiya. "On the Bloody Trail of Al-Shabaab Terror Attacks." Daily Nation, https://www.nation.co.ke/kenya/news/on-the-bloody-trail-of-al-shabaab-terror-attacks--842016. Accessed 1 Aug. 2020.

James C. Scott, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed* (New Haven: Yale University Press, 1998).

Kakah, Maureen. State barred from collecting DNA in 'Huduma Namba' Business Daily: Economy. April 1, 2019. https://www.businessdailyafrica.com/economy/State-barred-from-collecting-DNA/3946234-5052048-11jmn9v/index.html

Kenya Gazette Supplement, No. 167 (Acts No. 19). The Security Laws Amendment Act 2014.

Kenya Gazette Supplement. *The Statute Law (Miscellaneous Amendments) Act, 2018*. January 4, 2019. http://kenyalaw.org/kl/fileadmin/pdfdownloads/AmendmentActs/2018/StatuteLawMiscellaneousNo18of2018.pdf

Kenya High Court. Constitutional & Judicial Review Division: Consolidated Petitions No. 56, 58 & 59 Of 2019. January 30, 2020. http://kenyalaw.org/caselaw/cases/view/189189/

Kenya High Court. Constitutional and Human Rights Division: Consolidated Petitions No. 56, 58 & 59 Of 2019. http://kenyalaw.org/caselaw/cases/view/172447/.

Kimani, Trizah. "36 million registered for Huduma Namba" The Star. May 24, 2019. https://www.the-star.co.ke/news/2019-05-24-36-million-registered-for-huduma-namba/.

Migdal, Joel S. *State in Society: Studying How States and Societies Transform and Constitute One Another*, Cambridge University Press, 2001. P. 5 http://ebookcentral.proquest.com/lib/washington/detail.action?docID=201448.

Ministry of Interior & Coordination of National Government. *State Department for Interior and Citizen Services*. https://www.interior.go.ke/state-department-for-interior-citizen-services/.

Moore, Jina. "Cambridge Analytica Had a Role in Kenya Election, Too", New York Times, 20th March 2018 https://www.nytimes. com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html. Accessed July 9, 2020.

Muthuri, Robert et al. Biometric Technology, elections, and Privacy. CIPIT. 2017.

Mutisya, Musembi. The Huduma Number — Digital Identity and Inclusion in Kenya. June 7, 2019. https://pesacheck.org/the-huduma-number-digital-identity-and-inclusion-in-kenya-819ccdfd2ae0.

National Research Council (US) Whither Biometrics Committee; Pato JN, Millett LI, editors. Biometric Recognition: Challenges and Opportunities. Washington (DC): National Academies Press (US); 2010. 1, Introduction and Fundamental Concepts. Available from: https://www.ncbi.nlm.nih.gov/books/NBK219892/

Nyanjom, Othieno. 2011. "Devolution in Kenya's New Constitution." *Constitution Working*

Nyawira, Lyndsay. "All you need to know about the Huduma Namba." The Star. April 2, 2019. https://www.the-star.co.ke/news/2019-04-02-all-you-need-to-know-about-huduma-namba/. Accessed July 2019.

Onywoki, Benson M., and Dr Elisha T. Opiyo. *A Framework for the Adoption of Biometric Atm Authentication in the Kenyan Banks*.

Paper no. 4. Nairobi: Society for International Development. p.4

Petition 56, 58 & 59 of 2019 (Consolidated). http://kenyalaw.org/caselaw/cases/view/189189/

Planet Biometrics. EDAPS introduces biometric portal in Kenya. January 15, 2013. https://www.planetbiometrics.com/article-details/i/1430/

Privacy International. *Kenyan Court Ruling on Huduma Namba Identity System: the Good, the Bad and the Lessons*. February 24, 2020. https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons

Privacy International. *State of Privacy in Kenya*. 29 January 2019. Accessed November 2019. https://privacyinternational.org/state-privacy/1005/state-privacy-

kenya#:~:text=Once%20law%2C%20the%20Bill%20would,privacy%20of%20their%20communications%20infringed%E2%80%9D.

Privacy International. *Track, Capture Kill: Inside Communications Surveillance and Counterterrorism in Kenya*. 2017.

Regulation 15(1), the Kenya Information and Communications (Consumer Protection) Regulations, 2010.

Thales. Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Accessed June 12, 2020.

The Republic of Kenya. The National Intelligence Service Act, 2012. August 27, 2012. Access February 2020. https://www.nis.go.ke/downloads/THE%20NATIONAL%20INTELLIGENCE%20SERVICE%20ACT,%202012.pdf.

Wakaya, Jeremiah. "Kenyatta Merges Interior and Immigration Departments in Realigned Govt Structure" Capital News. August 29, 2019. https://www.capitalfm.co.ke/news/2019/08/kenyatta-merges-interior-and-immigration-departments-in-realigned-govt-structure/. Accessed August 11, 2020.

Wanyama, Jentrix. "CIPIT launches checklist on privacy and security in Kenyan legislations" CIPIT Blog. November 25, 2019. https://cipit.strathmore.edu/cipit-launches-checklist-on-privacy-and-security-in-kenyan-legislations-2/ Accessed July 2020.