Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights

Justin Bryant

24 STAN. TECH. L. REV. 389 (2021)

This Note argues that the contemporary data protection landscape on the African continent must be tailored to better address the needs of young, vibrant, entrepreneurial societies and resonate with the values therein. Toward this end, this Note issues recommendations aimed at creating effective legal and extralegal enforcement mechanisms. The implementation of these recommendations stands to position the continent well in the years to come and amplify the voices of African nations in the evolving global dialogue. Brief case studies from six countries are used to highlight the divergent development of data protection laws across the continent while simultaneously underscoring how common predominant influences—including past and present vestiges of colonialism—have left Africa short of effectiveness on this front. Following this is an analysis of the diverse obstacles faced by the public sector and the private sector. Then, a comparative law theory known as the "transplant effect" is introduced to explain impediments observed in the proliferation of data protection laws. Africa's place in global geopolitics is then highlighted, and the ways in which international players are exploiting Africa from a data privacy standpoint are addressed. Strategies for stakeholders to address threats while maximizing growth opportunities, including the UN Guiding Principles on Business and Human Rights, are evaluated in

context. Emphasis is placed on targeted action at the multinational, national, and local levels in order for societies to realize robust and comprehensive ecosystems that safeguard human rights and promote dignity in the digital space.

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

AU	AFRICAN UNION
BRI	BELT AND ROAD INITIATIVE
CNIL	COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (FRANCE)
DGL	DIGITAL GOVERNANCE LIAISON
DPA	DATA PROTECTION AUTHORITY
DPA 2004	DATA PROTECTION ACT 2004 (MAURITIUS)
DPA 2017	DATA PROTECTION ACT 2017 (MAURITIUS)
DPC	DATA PROTECTION COMMISSION
DPD	DATA PROTECTION DIRECTIVE
EAC	EAST AFRICAN COMMUNITY
EC	EUROPEAN COMMISSION
ECOWAS	ECONOMIC COMMUNITY OF WEST AFRICAN STATES
EU	EUROPEAN UNION
GDPR	GENERAL DATA PROTECTION REGULATION
GPS	GLOBAL POSITIONING SYSTEM
ICT	INFORMATION AND COMMUNICATION TECHNOLOGY
INAI	INSTANCE NATIONALE D'ACCÈS À L'INFORMATION (TUNISIA)
INPDP	INSTANCE NATIONALE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (TUNISIA)
ISP	INTERNET SERVICE PROVIDER
JP	JUSTICE OF THE PEACE
NDPR	NIGERIA DATA PROTECTION REGULATION
NITDA	NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NIGERIA)
OECD	ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
POPIA	PROTECTION OF PERSONAL INFORMATION ACT (SOUTH AFRICA)
SADC	SOUTHERN AFRICAN

	DEVELOPMENT COMMUNITY
SIM	SUBSCRIBER IDENTIFICATION MODULE
SMS	SHORT MESSAGE SERVICE
SOE	STATE-OWNED ENTERPRISE
U.K.	UNITED KINGDOM
U.N.	UNITED NATIONS
UNGP	UNITED NATIONS GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS
U.S.	UNITED STATES OF AMERICA

I. INTRODUCTION

In 2017, Africa outpaced all other continents in terms of internet penetration.[1] In Mali, the number of internet users in January 2018 was nearly 600% of what it was a year earlier. In the same period, Benin, Sierra Leone, Niger, and Mozambique saw their active internet users more than double.[2] Of the ten countries that experienced the highest growth in social media users from 2017-2018, four were located in Africa.[3] African internet bandwidth also saw a compound growth rate of 45% from 2014 to 2018.[4] It is clear that connectivity and technological development are accelerating and show no signs of slowing down in the near future. It is unclear, however, whether regulations governing the digital space will meet the needs of the next generation of digital users on the African continent.

Historical and contemporary trends in internet governance do not provide much cause for optimism. The General Data Protection Regulation (GDPR)[5] has quickly become the global standard for data protection

[1] Daniel Mumbere, *Digital in 2018: Africa's Internet Users Increase by 20%*, AFRICANEWS (Feb. 6, 2018), https://perma.cc/6PW9-Z4JV.
[2] *Id.*
[3] *Id.*
[4] Alan Mauldin, *International Internet Capacity Growth Just Accelerated for the First Time Since 2015*, TELEGEOGRAPHY (Sept. 20, 2018), https://perma.cc/A8LJ-XCQD.
[5] Council Regulation (EU) 2016/679 of the European Parliament and of the Council of

law since coming into effect in 2018.[6] The regulation emerged out of an acknowledgment in the European Union (EU) that the prior regulatory framework created by the Data Protection Directive (DPD) was insufficient to address growing threats to the privacy rights guaranteed to European citizens. The DPD had also allowed for incongruities among the data protection laws of EU Member States, which had become increasingly burdensome.[7] The impacts of the GDPR have been felt around the world, and it has been praised as a policy that aims to center users and their needs in the digital space. While this is admirable, the GDPR is ultimately a consensus around European norms and values—and the user that it centers is a European one. Far less often are the impacts of evolving data regulations discussed with an eye toward the developing world; never is the fastest-growing continent centered in the conversation surrounding global norms in the digital space.

A. Background

While globalization has created an interconnected and interdependent world economy, colonialism is the foundation of the inextricable economic ties between Europe and Africa, specifically. The EU is the largest trading partner of Sub-Saharan Africa, "accounting for 25.5 percent of imports and 23.2 percent of exports."[8] In terms of merchandise exports, African countries "trade twice as much with Europe as they do with each other."[9] Legal foundations laid during colonialism have undergirded this

27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[6] Foo Yun Chee, *Yet to Show Its Teeth, Landmark EU Privacy Law Already a Global Standard*, REUTERS (May 22, 2019), https://perma.cc/SX98-6U4K.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter DPD].

[8] Dhruv Gandhi, *Figure of the Week: Africa's New Trading Partners*, BROOKINGS (Mar. 7, 2018), https://perma.cc/TQC6-TVWQ.

[9] *African Countries Are Building a Giant Free-Trade Area*, ECONOMIST (Dec. 7, 2017), https://perma.cc/2YGX-5QJJ.

transcontinental economic activity. During "the entire colonial experience, indigenous peoples were forced to live with a particular system, either the continental civil codes or British common law. At independence, such experience of a national legal system as existed was of that designed by the continental European powers or the British."[10] Contemporary European laws no longer formally govern African nations, but in light of colonial history and present economic interconnectedness, it should come as no surprise that these societies still feel the impacts of EU legislation, and the national laws of certain EU Member States, as well as the United Kingdom.

Under the DPD framework that took root in the 1990s, Article 25 imposed an obligation on EU Member States to ensure that personal data relating to EU persons is covered by the laws of non-EU countries when it is processed in those countries.[11] The DPD was repealed upon passage of the GDPR, which, given its status as a regulation, became directly binding and applicable in the Member States. The new framework imposed by Article 3 shifted the responsibility for protecting the data of EU persons processed outside the EU from the Member States to the countries in which the processing occurs. Unlike DPD Article 25, GDPR Article 3 asserts that data controllers or processors "not established in the Union should also be subject to this Regulation" when their processing involves data subjects whose "behaviour takes place within the Union."[12] The penalties that can be leveraged on international entities for violating Article 3 have intensified the pressure on countries outside the EU to either adopt or approximate EU standards.

B. Colonial Influence in Regional Data Protection Schemes

Article 25 of the DPD allowed post-colonial blocs to serve as vehicles for European influence on data privacy standards in Africa. Conventions

---

[10] Sandra Fullerton Joireman, *Inherited Legal Systems and Effective Rule of Law: Africa and the Colonial Legacy*, 39 J. MOD. AFR. STUD. 571, 576 (2001).
[11] *See* DPD, *supra* note 7, at art. 25.
[12] GDPR, *supra* note 5, at art. 3.

such as the 2013 Francophone Binding Corporate Rules on cross-border transfer of personal data helped to harmonize the laws of France's former colonies in northwest Africa with those of France.[13] The Commission Nationale de l'Informatique et des Libertés (CNIL), the French data protection authority, has also made efforts to provide technical expertise and support to foster data privacy in these countries.[14] This is not an isolated phenomenon; Portuguese influence is seen within the data protection law of Cape Verde and its other former colonies as well.[15] While data protection legislation attempts to consolidate the responsibility to protect individual rights with the desire to enable commercial interests, it begs the question of whose rights and commercial interests are best served when laws are being imposed by a former colonial power. Do citizens resonate with the values these laws aim to promote? Are there carveouts to facilitate greater inclusion and growth of small business? Are appropriate sanctions in place to deter potential domestic and international violators?

C. Organizational Overview and Goals

Successfully adopting contextually sound data protection principles and interests in Africa will foster an environment in which regulations assist the proliferation of more progressive norms for the next generation of online users and provide African nations a voice in the global conversation. Failure to execute on this front may hinder the development of technology in Africa, infringe on individual liberties, and relegate African needs in the digital space to a secondary position in a firmly Western order. To explore this, we will first look at data protection laws that currently exist in Africa, discuss their origins, and see how these frameworks

---

[13] Cynthia O'Donoghue, *Francophone Data Protection Authorities Postpone Adoption of a New Framework for International Data Transfers*, TECH. LAW DISPATCH (Mar. 29, 2013), https://perma.cc/3997-37JM.

[14] *The CNIL Worldwide*, CNIL, https://perma.cc/2VNG-E6ZG (last visited May 5, 2021).

[15] João Luís Traça & Bernardo Emrby, *An Overview of the Legal Regime for Data Protection in Cape Verde*, 1 INT'L DATA PRIV. L. 249, 251 (2011).

integrate with legislation in other jurisdictions. We will profile several different countries, analyze particular trends, and zoom out to consider various challenges inherent to achieving effective digital governance across the continent. We will engage with literature on transplant effect and the difficulties associated with consolidating traditional values and everyday circumstances in Africa with the priorities of digital societies. Finally, we will observe how international players have exploited the current landscape of data privacy in Africa and consider a variety of strategies for stakeholders to address threats while maximizing growth opportunities.

II. LEGAL IMPACTS

A. Overview of African Data Protection Legislation: Convention Level v. Country Level

Over the last decade, there have been a series of multinational African conferences aimed at discussing continental standards for personal data protection and harmonizing norms across the region. These efforts have resulted in the formation of four data protection frameworks at the regional level and sub-regional levels: "The AU Convention on Cybersecurity and Personal Data Protection 2014, the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection, SADC Data Protection Model Law 2012[,] and the EAC Legal Framework for Cyber Laws 2008 (Phase I)."[16] The mid-2010s also saw the drafting of African Declaration on Internet Rights and Freedoms, which came together after a considerable degree of multi-stakeholder involvement. Despite these conversations and conventions, the desired impact of African regional and sub-regional privacy policies has yet to be realized. None of these policies have been ratified by a majority of states, so national legislation has been the centerpiece of efforts thus far.

[16] Alex B. Makulilo, *The Future of Data Protection in Africa*, *in* AFRICAN DATA PRIVACY LAWS 371, 377 (Alex B. Makulilo ed., 2016).

At the time of the writing of this Note, there are twenty countries in Africa with a comprehensive data protection law currently in effect and being enforced by a regulator. Roughly seventeen have laws that offer some such protections or comprehensive laws that have yet to become effective. While several countries have laws in draft stages, others have seen no legislative action in this area. The Part below will detail the circumstances that brought about data protection legislation in a few countries and address the critical provisions of their laws. Many provisions in the data protection laws of these countries are similar if not identical, given their origins in European statutes that in many instances have been directly transposed. To illustrate this, the first case study (Ghana) will focus more heavily on the text, structure, and foundations of the law; the examples that follow will be more geared toward the context and challenges of data protection law in that national environment.

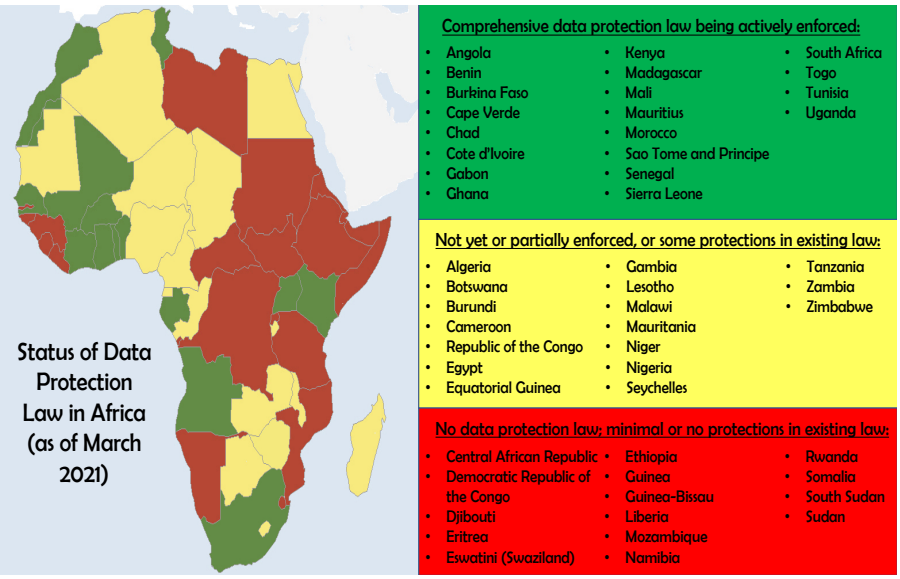

FIGURE 1

B. Selected Cases

1. Ghana

Ghana took significant steps in the realm of personal data protection in the 2010s in attempts to bring the country in line with global standards.[17] The Economic Community of West African States (ECOWAS), to which Ghana belongs, developed a framework for data protection law in April 2010, and Ghana was one of the first four African countries to sign onto the African Union Convention on Cybersecurity and Personal Data Protection 2014 (Malabo Convention).[18] In 2012, Ghana enacted the Data Protection Act (Act 843), a comprehensive piece of legislation that established principles and created an enforcement structure overseen by the Data Protection Commission of Ghana (DPC), which came into existence on November 18, 2014.[19] The DPC is charged with protecting "the privacy of the individual and personal data by regulating the processing of personal information, and . . . [providing] the process to obtain, hold, use or disclose personal information."[20]

Act 843 borrowed heavily from European regulations and Western multinational conventions. Section 96 defines processing essentially identically to Article 2(b) of the DPD, which became Article 4(2) of the GDPR.

Act 843 Section 96:

> . . . an operation or activity or set of operations by automatic or other means that concerns data or personal data and the (a) collection, organisation, adaptation or alteration of the information or data, (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission,

---

[17] *Id.*
[18] *Id.*
[19] Dominic N. Dagbanja, *The Right to Privacy and Data Protection in Ghana*, *in* AFRICAN DATA PRIVACY LAWS 229, 231 (Alex B. Makulilo ed., 2016).
[20] *Id.* at 240.

> dissemination or other means available, or (d) alignment, combination, blocking, erasure or destruction of the information or data.[21]
>
> DPD Article 2(b)/GDPR Article 4(2):
>
> . . . any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking ("restriction" in GDPR), erasure or destruction;[22]

Additionally, the eight Data Protection Principles outlined in Section 17 are directly modeled from the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[23] These principles comprise the core of Act 843:

i. *Under the Accountability Principle (AP), data controllers are required to ensure that data subjects' privacy rights are not infringed upon by using the data in a lawful and reasonable manner.*[24]
ii. *The Lawfulness of Data Processing Principle necessitates that personal data be processed only "if the purpose for which it is to be processed, is necessary, relevant and not excessive."*[25]
iii. *The Specification of Purpose Principle is designed to guarantee that personal data processing happens for specific purposes which must be, "explicitly defined and lawful" and related "to the functions or activity of the person" collecting the data.*[26]
iv. *The Compatibility of Further Processing Principle, detailed in*

---

[21] *Id.*
[22] GDPR, *supra* note 5, at art. 4.
[23] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, https://perma.cc/ANJ8-22NM (last visited Apr. 8, 2021).
[24] *Data Protection Principles*, DATA PROT. COMM'N (2020), https://perma.cc/Z6HC-5AJW.
[25] *Id.*
[26] *Id.*

Section 25, states that where personal data collected is held "in connection with a specific purpose, further processing of the personal data shall be for that specific purpose."[27]

v. *The Data Subject Participation Principle, found in Sections 20 and 21, states that personal data shall not be processed "without the prior consent of the data subject," and it requires direct collection of "personal data . . . from the data subject."*[28] *However, this provision allows for personal data to be obtained indirectly when the data is held in a public record, if the data subject has intentionally made the data public, or given consent to the collection of the data from another source.*

vi. *The Openness Principle extends from the Data Subject Participation Principle but goes further to emphasize "the need for the data subject to be made aware of the purpose for the collection of the data," and in Sections 32 and 33, gives data subjects the right to access and correct personal information.*[29]

vii. *The Data Security Safeguards Principle is reflected in provisions dealing with maintenance and retention of records, and these provisions establish that data should not be retained for longer than is reasonably necessary.*[30]

viii. *The Quality of Information Principle, detailed in Section 26, requires personal data controllers to ensure that personal data "is complete, accurate, up to date and not misleading having regard to the purpose for the collection or processing of the personal data."*[31]

Act 843 also contains enforcement provisions for violations of the Data Protection Principles. The DPC has the authority to send enforcement notices to data controllers upon evidence of a violation that has caused, "or is likely to cause damage or distress" to a person.[32] This notice may contain specific instructions for the data controller to rectify the violation, and if the data controller fails to comply, Section 80 stipulates penalties. Noncompliance with an enforcement notice may lead to a fine,

---

[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Dagbanja, *supra* note 19, at 244.

a term of imprisonment of no more than 1 year, or both.[33] Other enumerated offenses carry a fine or a term of imprisonment lasting no longer than two years, and certain unspecified violations can carry a fine of up to "5000 penalty units" (1 penalty unit ≈ 4 USD), and a prison term of up to ten years.[34] Individuals have a private right of action under Section 3, and under Section 43, damages are available for individuals who have suffered harm due to an infringement by a data controller.[35] Such individuals can also opt to file a complaint in court under Article 33(1) of the Constitution alleging that their right to privacy has been infringed upon.[36] It remains to be seen whether this dual structure of redress that does not necessarily require the DPC's involvement could render the body ineffectual.

Debate exists over the true impetus for the passage of Act 843. Certain scholars, as well as Ghanaian government officials, assert that the intention was "to give practical legal effect to the constitutional right to privacy of communication."[37] Edward Boamah, the Minister of Communications in 2014, said, "the underlying notion behind the codification of data protection is the ever growing need to process personal data today. Every Ghanaian has the right to the privacy . . . and such right must be guaranteed in the processing of his or her personal data irrespective of the medium used."[38] Another official voiced concern over how "the barrage [of] privacy invasions . . . [has] led to discrimination, personal harassments, damage to professional reputations, financial losses and in some extreme cases death."[39]

Nonetheless, others posit that economic considerations drove the enactment of Act 843 more than concerns about individual harms. While it is true that in the years leading up to the passage of Act 843, data breaches

---

[33] *Id.*
[34] *Id.*
[35] *Id.* at 245.
[36] *Id.*
[37] *Id.* at 230.
[38] *Id.* at 231.
[39] *Id.* at 232.

led to embarrassing scandals—some of which resulted in high-profile suicides—scholars point to the collectivist nature of Ghanaian and other African societies that have generally had low levels of privacy concerns, and attitudes did not seem to shift considerably in the years preceding Act 843.[40] Alex Makulilo argues that "a powerful driver of the development of privacy law among developing countries is the desire to engage in global e-Commerce and the recognition of trust as being a fundamental component of the new economy."[41] The near-identical language seen in Act 843 and EU statutes suggests that the drafters fully intended to satisfy European requirements for cross-border data flows. While Act 843 filled the void of substantive and procedural bases to protect the privacy of data and communications, one must wonder what specific carveouts and principles were adopted for the Ghanaian landscape if the Act truly intended to engage with events and attitudes within Ghana. The lack of unique substantive provisions suggests that the drafters did not sufficiently consider the challenges particular to the population.

2. Nigeria

Section 37 of the 1999 Constitution of the Federal Republic of Nigeria grants citizens the right to privacy.[42] The National Information Technology Development Agency (NITDA) attempted to translate this right into the domain of personal data in 2019 through the Nigeria Data Protection Regulation (NDPR), which went into effect on April 25 that same year. All public and private organizations that process personal data were required to publicize their NDPR compliant data protection policies and conduct initial audits of their privacy and data protection practices as of July 25, 2019. To address the particular difficulties public institutions

[40] *Id.* at 231-34.
[41] *Id.* at 232.
[42] Justin Bryant, *Nigeria*, DATA PROTECTION AFRICA (Mar. 31, 2020), https://perma.cc/FC48-5ZY8.

were facing, NITDA published guidelines in May 2020 to facilitate their compliance.[43]

While the principles in the NDPR may have been relatively standard, there were a number of structural failures in its passage that have since manifested. From the beginning, the NDPR was on questionable institutional footing within the structure of the Nigerian government. NITDA was tasked with the enforcement of the NDPR, and whether or not there was enough bandwidth within the organization to handle NDPR enforcement in addition to its pre-existing duties, NITDA is an executive agency with a narrow, statutorily-mandated scope. The NDPR is therefore limited to the powers granted to NITDA under the NITDA Act. NITDA cannot extend the scope of NDPR application to non-automated personal data or beyond natural persons residing in Nigeria or Nigerian citizens outside the nation's borders.[44] It also cannot create new roles and functions or exercise discretionary enforcement power. Particularly concerning is the fact that as a subsidiary legislation, the NDPR can be repealed by any act of Parliament.[45] This is why most countries that enact comprehensive data protection legislation create an independent regulatory body with its own mandate to enforce and oversee the regulation.[46]

It appears that the Nigerian government did not anticipate, nor intend for, these issues and is now seeking to rectify them. In March 2020, the government introduced a draft data protection bill, and the Legal and Regulatory Reform Working Group received comments from stakeholders in the months that followed.[47] The bill seeks to establish a DPC charged with responsibility for the protection of personal data, safe-

[43] Gabriel Omoniyi, *Actions: Beyond the Nigerian Data Protection Regulations (NPDR) 2019*, LEXOLOGY (Dec. 24, 2020), https://perma.cc/VN2D-HHF4.
[44] *Id.*
[45] Bisola Scott & Sandra Eke, Nigeria: *A Review of the Nigerian Data Protection Bill 2020*, MONDAQ (Sept. 8, 2020), https://perma.cc/LWN9-UR4G.
[46] Bryant, *supra* note 42.
[47] FEDERAL REPUBLIC OF NIGERIA ET AL., INVITATION TO COMMENT ON THE DRAFT DATA PROTECTION BILL, 2020 (2020), https://perma.cc/7B2D-RMCD.

guarding the rights of data subjects, and regulating the processing of personal data.[48] The objectives of the bill include promoting a code of practice that ensures the privacy and protection of data subjects, minimizing harmful effects of personal data misuse, and ensuring that personal data processing occurs in a transparent, fair and lawful manner per the provisions of the bill and other laws of the nation.[49] When passed into law, this bill may finally bridge the gaps that exist in the regulatory regime.[50]

3. Tunisia

Tunisia was one of the first movers in Africa in terms of data protection legislation, but these early efforts proved to be hollow. Two years after updating its 1959 Constitution to include the right to personal data protection in 2002,[51] the Ministry of Justice advanced the Organic Act No. 2004-63, which established the Tunisian data protection authority, the *Instance nationale de protection des données à caractère personnel* (INPDP).[52] Under Organic Act No. 2004-63, data subjects have the right to:

- access all personal data concerning them[53]
- correct, complete, rectify, update, modify, clarify, or delete when the data is inaccurate, equivocal, or when its processing is prohibited[54]

[48] Omoniyi, *supra* note 43.
[49] *Id.*
[50] Scott & Eke, *supra* note 45.
[51] Justin Bryant, *Tunisia*, DATA PROTECTION AFRICA (Mar. 31, 2020), https://perma.cc/9VMC-BDP5.
[52] *Id.*
[53] *Id.*
[54] *Id.*

- object, at any time, to the processing of personal data concerning him for valid, legitimate, and serious reasons, except where the treatment is planned by law or is required by the nature of the obligation[55]

- prevent personal data from being shared with third parties for advertising purposes[56]

These steps should have made Tunisia one of the most progressive regimes for personal data protection in the world, but under the authoritarian rule of Ben Ali, few, if any, of the rights guaranteed in these laws, were actually realized by the people. The Jasmine Revolution of 2011 brought democratic reforms, but it wasn't until 2015 that data processors began to regularly declare their personal data processing to the INPDP. Even if data processors had been doing their part, it would have been in vain; the INPDP was not functioning as an independent body, nor was it sanctioning violators of the Organic Act.

Tunisia ratified a new constitution in 2014, but the old data protection regime remains.[57] During a 2018 conference, Chawki Gaddes, president of the INPDP, emphasized the importance of modernizing the law toward greater effectiveness, and to reflect new social and technological realities as well Tunisia's new political environment that values democracy and human rights.[58] The obligations that generally apply to personal data processors in Tunisia do not apply to organizations with a "public personality" (such as police stations, tribunals, and universities).[59] Because public sector bodies are not required to declare data processing, the rights of individuals with regards to their data are limited in their interactions with these entities.

---

[55] *Id.*

[56] *Id.*

[57] *See* Tunisia's Constitution of 2014, https://perma.cc/98Q7-WKLH (last visited May 5, 2021).

[58] Emna Sayadi et al., *As Elections Approach, Tunisia Must Ensure Protection of Personal Data*, ACCESS NOW (Aug. 16, 2019), https://perma.cc/CY7V-LAYA.

[59] Bryant, *supra* note 51.

Similar concerns surrounding public sector accountability were expressed in a report from the Tunisian Access to Information Authority (*Instance Nationale d'Accès à l'information*, INAI) about a 2018 draft law intended to update the current regime. In not distinguishing between the personal data of individuals related to their private lives and those relating to public life or to the management of public affairs, the draft law, the INAI wrote, "violates the principles of transparency and access to information guaranteed by the Tunisian Constitution."[60] Given the trends of public sector abuse of personal data being observed globally, but particularly within Africa, it is critical to close these gaps that foster distrust between citizens and their governments.

4. South Africa

In 2001, South Africa first appointed a committee to investigate the state of privacy and data protection and consider a legislative framework, and eight years later, the Protection of Personal Information Act (POPIA)[61] was drafted.[62] In 2013, Parliament adopted it into law with no implementation timeline, but certain provisions took effect over a number of years, and as of July 1, 2020, the regulation is in full effect. Responsible parties were given until July 1, 2021 to reach full compliance.[63]

---

[61] In the patchwork of laws across different countries, as well as in common parlance, the terms "data" and "information" are used interchangeably. The reader is advised to disambiguate these terms and not to conflate them, as they are not identical. While the definitions are not entirely set, one may find the following explanation illustrative: "Data are recorded (captured and stored) symbols and signal readings [. . .] Information is a message that contains relevant meaning, implication, or input for decision and/or action. Information is a message that contains relevant meaning, implication, or input for decision and/or action [. . .] Knowledge is the (1) cognition or recognition (know-what), (2) capacity to act (know-how), and (3) understanding (know-why) that resides or is contained within the mind or in the brain." Anthony Liew, *Understanding Data, Information, Knowledge and Their Inter-Relationships*, 7 J. KNOWLEDGE MGMT. PRAC. 1, 5 (2007).

[62] Anneliese Roos, *Data Protection Law in South Africa*, *in* AFRICAN DATA PRIVACY LAWS 189, 201 (Alex B. Makulilo ed., 2016).

[63] *Id.* at 200.

POPIA was created with the stated purpose of being, "in harmony with international standards," when protecting personal information when processed by public and private bodies.[64] POPIA contains eight conditions for lawful data processing: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.[65] These conditions are nearly identical to the Data Protection Principles in Ghana's Act 843, and are derived from the Council of Europe Convention, the EU's DPD, and also the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Additionally, POPIA established the Office of the Information Regulator and since 2016, this body has been enforcing the effective components of the regulation.[66]

Throughout the long process of bringing POPIA into effect, the GDPR emerged. South African businesses that were preparing for new domestic regulations in 2016 suddenly needed to comply with European ones as well. While auditing and improving data protection practices has likely facilitated compliance across the board, the GDPR and POPIA are different in several ways. Despite the larger fines for violations of the GDPR, there are no criminal offenses under the regulation, which is not the case under POPIA, where violations can carry fines of up to 10 million ZAR (~667,000 USD) and a maximum prison sentence of ten years for the executives of violating entities. Despite the ample time that companies have had to move toward compliance, research from a South African marketing agency, Rogerwilco, "indicates that only 25 percent of South Africa's most popular websites have pop-ups that explicitly ask visitors for consent to collect data about their browsing activity."[67] It remains to be seen how strictly violations will be punished when the grace period expires.

---

[64] Roos, *supra* note 62, at 203.
[65] *Id.*
[66] *Information Regulator in South Africa*, MICHALSONS (Jan. 3, 2021), https://perma.cc/4T8D-P97W.
[67] *75% of SA's Top Websites Risk R10m Fines for Popi Non-Compliance - Rogerwilco*, IOL (June 30, 2020), https://perma.cc/N93R-UH4C.

5. Mauritius

As a small island country, Mauritius sees attracting critical foreign investment and facilitating data flows with European business partners as the primary reasons to keep its data protection framework current and aligned with European standards.[68] When Mauritius enacted the Data Protection Act of 2004 (DPA 2004), it became the first African country to establish the office of the Data Protection Commissioner and make it operational.[69] The DPA 2004 was largely based on the EU's DPD, and was amended in 2009 to rectify concerns around the Commissioner's powers of entry and search in Section 17. It also repealed the contentious Section 21 which gave the Prime Minister the authority to give the Data Protection Commissioner direction in the discharge of his duties. Chief among the motivations for the amendments was "the need for Mauritius to be potentially recognized by the European Union as a third country with an adequate level of protection and thus attract more investment in . . . the Information Technology Enabled Service/Business Process Outsourcing sectors."[70]

Mauritius was the first country in the Southern Hemisphere to revamp its regulatory regime by repealing the DPA 2004, and adopting the DPA 2017 following the passage of the GDPR.[71] The most significant changes between the DPA 2004 and the DPA 2017 were the implementation of data protection impact assessments, notification of personal data breach, stricter security requirements attached to data processing, and clearer standards around the details of lawful processing.[72] Mauritian leaders attest that, "a stronger and more coherent data protection framework, backed by effective enforcement will allow the digital economy to

---

[68] Melissa Virahsawmy & Vishwanee Boodhonee-Aikat, *Mauritius: Mauritius Updates Its Data Protection Legislation to Be in Line with GDPR*, MONDAQ (Mar. 26, 2018), https://perma.cc/8QTB-JVPF.

[69] Alex B. Makulilo, *Data Protection of the Indian Ocean Islands: Mauritius, Seychelles, Madagascar*, *in* AFRICAN DATA PRIVACY LAWS 277, 282 (Alex B. Makulilo ed., 2016).

[70] *Id.* at 283.

[71] Virahsawmy & Boodhonee-Aikat, *supra* note 68.

[72] *Id.*

flourish by putting individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities."[73]

6. Angola

Angola's National Assembly passed Law 22/11 on Personal Data Protection on June 17, 2011.[74] It is an omnibus data protection law that "applies to the automated and non-automated processing of personal data by controllers based or operating in Angola, or subject to, or using equipment governed by, Angola's laws."[75] The Law creates a data protection agency called the *Agência de Proteção de Dados*, and it was announced on October 9, 2019 that the agency had become operational.[76] Given this, enforcement of Law 22/11 is at a very early stage.

Provisions within the Law draw from both the EU's DPD and the Portuguese legal regime for the protection of personal data. Under Law 22/11, "all data processing operations must respect general principles of transparency, lawfulness, [and] proportionality."[77] Law 22/11 establishes specific categories of personal data and stipulates additional rules for the processing of certain kinds of sensitive data. The Law differs from the data protection legislation of other countries in that it focuses on personal data processing connected to Angolan territory, rather than Angolan persons, which likely creates a narrower scope of protection. For personal data to fall under the umbrella of Law 22/11, the data must have been 1) processed "by a data controller based in Angola; 2) in the course of the activities of a data controller based in Angola, even where the data controller does not have its head office there; 3) anywhere outside of Angola where Angolan law applies as a result of public or private international

[73] *Id.*
[74] *Angola Passes Personal Data Protection Law*, PRIV. & INFO. SEC. L. BLOG (Sept. 19, 2011), https://perma.cc/3LE6-SPQ7.
[75] *Id.*
[76] *Angola*, ONETRUST DATAGUIDANCE (2020), https://perma.cc/V68X-GZ3X.
[77] João Luís Traça & Francisca Corriea, *Data Protection in Angola*, *in* AFRICAN DATA PRIVACY LAWS 349, 353 (Alex B. Makulilo ed., 2016).

law; or 4) by a data controller located outside of Angola through any means located in Angolan territory."[78] Additionally, the maximum penalty that the law imposes for failure to comply is 150,000 USD, which, depending on how these penalties are allocated, could be insufficient to deter large-scale violations from big tech companies.[79]

C. Compliance Challenges

While country-level legislation on data protection is being enacted in Africa, it is important to remember that most African countries still do not have comprehensive legal frameworks for data protection, and those that do face considerable obstacles in enforcement. As major gaps exist in Africa's data privacy landscape, challenges will persist for years to come.

1. Public Sector: Policy Enforcement Failures

Adequately governing public sector management of personal data is a common struggle for jurisdictions around the world. The public sector has a different relationship with individuals than the private sector, and the nature of the services governments provide may require government entities to retain sensitive data on individuals for extended periods of time. Public sector organizations have various points of intersection and serve many diverse functions but generally must abide by similar protocols across agencies. Government agencies are difficult to penalize, and institutional failures in public sector institutions are rarely addressed until harms substantial enough to merit public outcry have already transpired—assuming one's government is accountable to the public at all.

In several African countries, public sector organizations are among the most flagrant misusers of personal data. Governments have gained access to advanced technologies before their regulations have specified

[78] *Id.* at 352.
[79] *Id.*

guidelines for proper use and limitations, opening the door for widespread abuse. Even where laws are codified, certain privacy norms may not resonate with authorities. For example, in Kenya in 2017, the Communications Authority requested that telecoms Safaricom, Airtel, and Telkom Kenya install Data Management Systems to detect fake mobile devices.[80] The Communications Authority had "switched off 1.5 million fake mobile phones in 2012" but wanted this additional tool to completely eradicate the problem. This decision reached the High Court, where a judge rejected the plan, convinced that the installation of the Data Management Systems "was an infringement on mobile subscribers' privacy."[81] In this case, the court system proved to be an effective vehicle for rights enforcement in advance of a major potential violation. However, regulation regularly lags behind innovation and there are many examples of scenarios in which advanced technologies were deployed and caused extensive harm to communities before courts were able to get involved.

Inadequate protection of biometric data poses significant problems across the continent. Several countries have experimented with creating databases populated with biometric data without giving proper weight to the privacy interests at stake. In 2011, the Nigerian Communications Commission began a project to fight identity fraud and bolster public safety by mandating that local telecommunications operators register all existing and newly issued SIM cards.[82] This endeavor took several years and involved the collection of biometric data from tens of millions of mobile users.[83] One of the goals of this program was to create a national identification database that could be centralized and utilized by other government agencies.[84] However, a lack of streamlined standards and

---

[80] Kamau Muthoni, *Blow to CA Court Blocks Plan to Snoop into Mobile Phones Conversations*, STANDARD (Apr. 20, 2018), https://perma.cc/66PA-S5JW.
[81] *Id.*
[82] Omo Osagiede, *Why Africa's Private Sector Should Be Concerned About More Than the GDPR*, CSO (June 6, 2018, 5:57 AM), https://perma.cc/JCU4-ZKWT.
[83] *Id.*
[84] *Id.*

policies created a scenario in which these agencies each established their own national identification projects in isolation, collecting much of the same data that had already been collected in the original project.[85] Furthermore, phone-related crime remains a problem in Nigeria, so the registration was a failure from that angle as well.[86]

The volumes of biometric data that Nigerians have volunteered to various agencies for the purposes of doing things such as obtaining passports, drivers' licenses, and bank verification is even more alarming. Despite Section 37 of the Nigerian Constitution guaranteeing citizens a right to privacy, these highly invasive projects were launched with virtually no transparency regarding the "collection, use, accuracy, storage, and transfer of sensitive biometric data from both data controllers and processors," and in the absence of a regulatory framework to protect citizen data (Nigeria only issued its national data protection regulation in late January 2019).[87] Following allegations that the Kenyan Independent Electoral and Boundaries Commission misused biometric data collected during the 2017 general elections, researchers at Strathmore University issued a report expressing that when technologies such as biometrics, "are adopted in the absence of a strong legal framework and strict safeguards, they pose significant threats to privacy and personal security, as their application can be broadened to facilitate discrimination, social sorting and mass surveillance."[88]

These threats have already manifested in Kenya, Zimbabwe, and several other African countries. Governments have installed camera systems with facial recognition software in attempts to use artificial intelligence to combat urban crime. The police force in Kampala, Uganda, says their

---

[85] *Id.*

[86] *See* Taiwo Ojoye, *NCC Should Get Tough on Unregistered SIMs*, PUNCH (Nov. 13, 2017), https://perma.cc/GCU5-RBJA ("The Executive Vice-Chairman of the NCC, Umar Dambatta, at an emergency meeting he held with representatives of the telecommunications companies in Abuja, rightly outlined the enormity of the threat posed by anonymous or improperly registered SIMs.").

[87] Osagiede, *supra* note 82.

[88] Betty Murithi, *New Report: Biometric Technology, Elections, and Privacy in Kenya*, STRATHMORE UNIV. (May 9, 2018), https://perma.cc/YTU8-SK3Y.

camera system has made the city safer and is "transforming modern day policing."[89] Civil society stakeholders feel otherwise. Dorothy Mukasa, executive director of Unwanted Witness, a nonprofit body that advocates for uncensored online platforms in Uganda says, "this should be concerning to every Ugandan. This is part of a wider surveillance in public spaces . . . . The key concern is we have no safeguards here. This is unregulated and there is a lack of accountability and transparency when it comes to collection of personal data."[90]

Even in countries with data protection law on the books, governments are attempting to enact policies that allow for broader surveillance capacities that run counter to data privacy interests. In 2016, the Ghanaian Parliament sought to rapidly advance a new surveillance bill that would have enabled the collection of massive amounts of personal data.[91] Groups such as Privacy International and ARTICLE 19 issued submissions against the passage of the bill to Parliament before it was ultimately defeated.[92] Despite the standards that the South African government enacted in POPIA, in 2017, a security researcher discovered a backup file that was actually a database that held the personal data of a large percentage of South Africa's population, including their National IDs, which can easily be decoded to derive more personal information.[93] These are just a few examples of how governments that establish bodies for regulation and enforcement of data protection often contravene these efforts.

2. *Private Sector: Strategizing in the Face of Uncertainty*

Robust data protection policies on the country level can support the goals of African-based multinational organizations. As businesses scale

---

[89] Tom Wilson & Madhumita Murgia, *Uganda Confirms Use of Huawei Facial Recognition Cameras*, FIN. TIMES (Aug. 20, 2019), https://perma.cc/L7BF-LUYD.
[90] *Id.*
[91] *Ghana: Parliament Needs to Rethink Controversial New Spy Bill*, ARTICLE 19 (Mar. 15, 2016), https://perma.cc/5LTZ-N6L7.
[92] Osagiede, *supra* note 82.
[93] Troy Hunt, *Questions About the Massive South African "Master Deeds" Data Breach Answered*, TROY HUNT (Oct. 19, 2017), https://perma.cc/SK6J-K9WD.

up and intersect with diverse global regions, they will be subject to extra-territoriality requirements such as those found in Article 3 of the GDPR, as well as the data protection laws of wherever their consumers may reside. "[N]on-compliance with personal data protection legislation could impede an organisation from transferring personal data cross-border, thereby hindering its business operations," and as international transactions are highly common, compliance is essential to secure business opportunities.[94]

Established companies are being advised that close compliance with the GDPR creates trust and reliability with their international consumers, given that many see the GDPR as the highest existing global standard for personal data protection.[95] Certain stakeholders in South Africa have recommended that Parliament amend POPIA to adhere more closely to the GDPR, for the Information Regulator to interpret POPIA in such a way that makes it more in line with GDPR requirements, or for her to issue additional requirements that are in line with the GDPR.[96] While these prescriptions might seem reasonable in the short run, in the long term, these actions would cede leadership and advancements in this realm to Europe. South African businesses dependent on the European market are compelled to adhere to European standards, but South African data protection law should reflect the needs of the totality of South African society. If trust and reliability with consumers is what companies aim to foster, they should heed their consumers' feedback concerning existing data privacy practices, and actively solicit information on changes they may wish to see. As end users become more sophisticated, private sector players should want their governments to be more responsive, and as such, they should encourage the passage of business-friendly legislation with both global and local salience.

---

[94] DELOITTE, PRIVACY IS PARAMOUNT: PERSONAL DATA PROTECTION IN AFRICA 3 (2017), https://perma.cc/PT5S-F576.

[95] Chee, *supra* note 6.

[96] John Giles, *GDPR vs POPIA*, MICHALSONS (Feb. 13, 2020), https://perma.cc/M3PP-49LM.

The GDPR did foresee the disparate impact compliance with data privacy laws poses within the private sector. The costs are more easily internalized by large, established companies, and can pose considerable challenges for smaller and emerging companies with fewer resources. GDPR Recital 13 acknowledges this problem, stating:

> To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping.
>
> In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.[97]

This provision, albeit aimed at easing burdens for small business, is unclear about what kinds of exceptions from the law that they may be entitled to, and therefore does little to alleviate uncertainty for firms allocating scarce resources. As countries seek to tailor data protection frameworks, the small business context could be a key area for new data protection legislation being drafted in African countries to provide instructive statutory guidance for jurisdictions across the world. The Internet Society's Personal Data Protection Guidelines for Africa encourage emerging companies to employ "Privacy by Design (PbD) and value-based design, as an integrated part of product/service development."[98] Technology attorneys advise startups to engage in data asset mapping and to consider "the most significant ways in which they process personal information within the organisation as well as externally," as well as immediately destroying information that is no longer relevant.[99] While

---

[97] GDPR, *supra* note 5, at Recital 13.
[98] *Personal Data Protection Guidelines for Africa*, INTERNET SOC'Y (May 8, 2018), https://perma.cc/EM2B-JXE7.
[99] Daniel Mpala, *€20m Fines Could Hit African Startups That Fall Foul of New EU Data Rules*, VENTUREBURN (May 2, 2018), https://perma.cc/AR7T-RMZ6.

these are helpful tips, they are quite general, and there is an opportunity for partnerships between small businesses, researchers, and public sector entities to collaborate on guidelines that could have a degree of universal application.

Technology evolves before regulation can respond, and this is a major challenge. GDPR and its deletion requirements were conceived of in a world that predated immutable ledgers. Workarounds have had to emerge such that innovations in the blockchain space were not simply made illegal and to remove certain obstacles for entrepreneurs. However, these unsettled areas of law provide companies with opportunities to take risks that can inform regulatory bodies. Rather than trying to approximate standards that are quickly becoming outdated, African governments should craft their data protection regulations to meet the technical and business challenges observed in their respective countries and in the world. If African businesses seek to manage the challenges of personal data protection by innovating on better technical and procedural measures, technologists, businesspeople, and policymakers can come together to create regulatory environments informed by country-specific use cases. This approach will be far more responsive to domestic needs and contribute to the creation of international standards.

III. SOCIETAL IMPACTS

A. Transplant Effect and Consequences of the Status Quo

The pressure for African societies to import or approximate the European data protection regime illustrates a scenario that is as familiar as it is novel. Notions of privacy are highly culturally contextual, and in order to garner the essential buy-in from the society, laws that govern this domain should be built out of norms and circumstances that resonate with locals. To be well-positioned as technological development accelerates on the continent, the regulatory foundations African nations put in place cannot simply be a collection of foreign "best practices," but must

be intentionally designed to consolidate traditional values with contemporary goals.

The difficulties that have been observed in the adoption and enforcement of data protection law in Africa can be largely explained by a comparative law theory known as the "transplant effect," which asserts that when laws are imposed on a population unfamiliar with them, "initial demand for using these laws [will] be weak. Legal intermediaries [will] have a more difficult time developing the law to match the demand . . . [and] their legal order [will] function less effectively than [those countries] that either adapted the law to local conditions and/or had a population that was familiar with the transplanted law."[100] This theory draws on an argument made by political economist Daniel Berkowitz, that "institution building should take into account local knowledge, and should not over-emphasize best practice blueprints observed in developed countries at the expense of local participation and experimentation," because "internal development can take advantage of new solutions economic agents develop in response to new challenges and existing constraints."[101]

The GDPR centers European persons and is based on notions of privacy that resonate with Westerners.[102] It was designed for a socioeconomic context unfamiliar to most Africans and comes on the shoulders of decades of iteration and discussion about the needs of Europeans in a rapidly developing world, as is demonstrated by the shift from the DPD to the GDPR. The Western individualism that is central to the conception of privacy and how it should be protected by institutions is unlikely to

---

[100] Daniel Berkowitz et al., *The Transplant Effect*, 51 AM. J. COMP. L. 163, 168 (2003).
[101] *Id.* at 169-70. *See generally* Dani Rodrik, *Institutions for High-Quality Growth: What They Are and How to Acquire Them* (Nat'l Bureau of Econ. Rsch., Working Paper No. 7540, 2000), https://perma.cc/CR4D-GU3T.
[102] *See* Cécile Georges, *GDPR: One Year on and Looking Ahead*, ITPROPORTAL (Nov. 21, 2019), https://perma.cc/3BEW-PJK7 ("Despite its Eurocentric focus, GDPR has had a huge impact in places like the USA where it has provoked a discussion around the need for privacy rights for individuals as opposed to just protecting specific types of data.").

map neatly onto societies in which a blend of individualism and collectivism characterize their cultures; this blend should be reflected in their laws. Wholesale exports of European policy, regardless of the rationale, are likely to result in enforcement failure.[103] This is not to say that there is no place for borrowing specific statutory provisions; some practices do not present cultural tension and can be universally recognized as good policy. Nonetheless, effective statutes tend to be rooted in and well-adapted to specific country contexts. They are built upon norms citizens already subscribe to and draw from the perspectives of diverse stakeholders. In 2018, the Internet Society and the Commission of the African Union embarked on a joint initiative to create the Personal Data Protection Guidelines for Africa.[104] Of the eighteen recommendations promulgated, eight discussed "[m]ulti-stakeholder solutions," the "[w]ellbeing of the digital citizen," and "[e]nabling and sustaining measures."[105] This demonstrates how institutions are recognizing the critical nature of local salience for policy development surrounding digital environments.

A lack of culturally-centered policy development in the data privacy space in Africa has also contributed to apathy and ignorance about its importance. In surveying Ghanaians on their concerns about privacy issues, scholar Eric Agyei-Bekoe found that his interviewees generally lacked "awareness and understanding of privacy and data protection issues."[106] Other studies by the World Wide Web Foundation and the Paradigm Initiative have shown that even where laws are on the books, "data subjects are often unaware of their privacy rights or are unaware of options for recourse in situations where their rights and freedoms have been abused."[107] Beyond a lack of awareness, it appears that data privacy is simply not a priority for the everyday person; Agyei-Bekoe's research also found

[103] Berkowitz et al., *supra* note 100, at 171.
[104] INTERNET SOC'Y, *supra* note 98.
[105] *Id.*
[106] Dagbanja, *supra* note 19, at 235.
[107] Osagiede, *supra* note 82.

"low privacy concerns among [his sample of Ghanaians], which are influenced by the national culture, specifically collectivist cultural society."[108]

Some argue that people in the developing world are facing more tangible and urgent socioeconomic issues, making concerns about data privacy largely unimportant.[109] However, structural socioeconomic concerns and data privacy concerns should not be mutually exclusive. Africans cannot afford to ignore the present threats of data mismanagement and exploitation. The scope of harm posed by these threats will increase in tandem with the scope of technological capabilities, and now is the time to identify and combat these threats before their scale and severity reach a point of no return. Arthur Gwagwa, a senior researcher at Strathmore University, recognizes that Africa's delays "when it comes to innovating around and addressing privacy issues" have become a serious liability in an era in which states can surveil and censor data traffic for self-serving purposes.[110] Civil society groups can help fill the void by offering public information campaigns and educational initiatives to bring issues of data privacy and technological abuse to people's attention. However, this is no substitute for rule of law. As digital penetration grows on the African continent, so should enforceable legislation that responds to the realities faced by the public.

B. Creating Community-Based Models for Norm Diffusion

To mitigate the obstacles posed by the transplant effect, strategies to implement data protection laws in African countries should include measures to adapt the law to local conditions and/or increase familiarity with the law, "and induce an internal process of law development and to generate a self-sustaining demand for legal innovation and change."[111]

---

[108] Dagbanja, *supra* note 19, at 235.
[109] *See* Dahir, *supra* note 88.
[110] *Id.*
[111] Berkowitz et al., *supra* note 100, at 190.

Beyond legislation, guidance and input at the community level is essential to creating a culture favorable to the protection of data and other individual rights. While the continent is rapidly urbanizing, most Africans still live in rural areas, and it is especially important to give voice to these perspectives. The development of a system of Digital Governance Liaisons (DGLs) could consolidate principles in legislation with the realities of communities, harmonizing top-down and bottom-up approaches. A longstanding British institution (that has now become mostly ceremonial) known as the Justice of the Peace (JP) might serve as a potential model for such a system. The JP endured for centuries in the U.K. because of its capacity to adapt to changes in the sociopolitical landscape over time, the respect and trust citizens place in the Justices, its low cost to the Crown, and the way in which it complemented other administrative councils and bodies that dealt with various initiatives over the years.[112] Particularly for rural residents, the JP was someone to whom people were comfortable voicing grievances, as he or she was responsible for advocating for the needs of the community.

1. Structure, Relationship to Stakeholders, and Responsibilities

DGLs would ideally be organized under a national Data Protection Authority (DPA) or another ministry tasked with overseeing digital policy. While the JPs were allowed a considerable degree of autonomy, their role was legitimized by a central government that gave overarching direction and support when necessary. Likewise, the DGL model will flourish best where a country has national comprehensive data protection legislation and a functioning DPA to which DGLs are connected so they can receive updates and be responsive to inquiries. Additionally, DPAs

---

[112] *See generally,* ESTHER MOIR, THE JUSTICE OF THE PEACE (Penguin Books 1969). In the same way that ineffectiveness often results when foreign legislation is transplanted into third-country legal codes, one could assume a similar trend for social institutions. In presenting the JP, I aim to provide an example from which stakeholders can choose aspects that map well onto their existing customs and community governance methods and consider how to create a system to defend digital rights on the community level.

should hold meetings in which DGLs can learn about the DPA's priorities for legislative enforcement and where the DPAs can receive relevant feedback from the DGLs. This would facilitate the DPA's ability to keep regulation up to date with technological innovation, as DPAs can usually issue instructions explaining how existing law will be enforced and propose amendments to lawmakers on a regular basis.

Countries will have to determine how much enforcement power to allocate to their DGLs as the role of a DGL will vary in different contexts. In countries where rule of law and governance channels are well-established, central government legislation may reach and take root in localities faster without the need for an additional layer of government bureaucracy. In such countries, a DGL may function more as an advocate for community concerns and be allocated few if any obligations around enforcement. However, in a country with many new internet users, or where legislation from the central government may face obstacles in reaching distant communities, a DGL may need to act more as an officer of the DPA and ensure the law is being faithfully followed. Here, similar to the JPs, DGLs should be given a degree of autonomy over their enforcement power based on what is feasible for their communities and the values that resonate there.

2. *Selection and Training*

In any case, this system relies entirely on the DGLs utilizing their superior knowledge of local dynamics unselfishly and toward the correct aims. For most of their existence, JPs were chosen from the landowning class of citizens.[113] Because of this, it is conceivable that their interests—which were often tied up in their property—may have kept them from enforcing certain laws or enforcing them in ways favorable to the preservation of their lands. Creating proper incentives for DGLs is critical, as it is not hard to see how corruption could undermine the integrity of this

[113] *History of the JP*, QUEENSLAND JUSTICES ASSOCIATION (2021), https://qja.com.au/history/.

system. Large, wealthy internet corporations, and even certain smaller players with specific goals, may try to influence DGLs if the system does not suit their interests. The potential for bribery would have to be considered when building such a system, as corporate interests could certainly pay DGLs better than DPAs. Adverse incentives could be countered through the imposition of term limits, although there may be downsides and risks posed by the lack of continuity. It could also be difficult in certain communities to find new people to fill the post each year, and this could introduce an undue administrative burden on the DPA. Nonetheless, the idea is to limit the potential for someone chosen as a DGL to exploit his constituents in any way. A selection process that achieves the requisite aims is worth considering in greater detail.

Training should be mandatory for DGLs as well. Ideally, they should have to pass an exam based on the data protection law of their country, as these individuals will need to be properly qualified to handle relevant data, address grievances on site, and faithfully represent matters to the DPA. Apart from training prior to the job, continual education is crucial when handling such dynamic matters. The JPs held Quarter Sessions, which were quarterly meetings with other JPs in their area to discuss and share ideas about governing.[114] DGLs should hold similar meetings to stay abreast of the concerns that other communities are facing on the data protection landscape so they can learn from the experiences of their peers.

3. Challenges and Limitations

Many challenges would accompany the introduction of DGLs. As the U.K. evolved over the years, so did the JP system, but it was able to do so as the institution was birthed in the U.K. and became embedded in that society over time.[115] Implementing a new institution takes considerable

---

[114] *Quarter Sessions*, ENCYC. BRITANNICA, https://perma.cc/MPA4-ZT2V (last visited May 3, 2021).
[115] *Justice of the Peace*, ENCYC. BRITANNICA, https://perma.cc/BH8X-DGSZ (last visited May 3, 2021).

buy-in from stakeholders, and the institution must latch onto familiar elements and values within the society.

Defining the relevant communities would be a considerable task. Precolonial societies across Africa were organized in many different ways, and the contemporary divisions are far from neat and clear. Additionally, the discussion thus far has presumed that DGLs will oversee a physical community. To what extent might it make sense to base this framework around digital communities, and how does that change how we consider this model? While it may be safe to presume that central authority comes from the nation-state, there may be advantages in thinking about different ways to frame the local, given that these days, one's online presence may be more stable than one's physical presence, and the latter need not necessarily affect the former.

Along with these questions of scope, logistical questions arise as well. What data sources, data points, and levels of access will DGLs be given? How will the data of community members be adequately protected from DGLs, and who will bear the responsibility for doing that? Will it be as simple as creating a secure upload platform that redacts and anonymizes data for concerns related to personally identifiable information, or is this too heavy-handed an approach? Furthermore, if DGLs are to have short tenures to mitigate against corruption, are stakeholders willing to invest the requisite resources to train them properly?

Like the JPs, DGLs will be administering existing laws, and perpetuating their native regime. The impact DGLs have in a society will likely reflect the mission of leadership from which they derive their mandate. In the context of autocratic rule, DGLs could potentially serve to further entrench the objectives of oppressive governments. Beyond this, when we consider the needs of internet users today, the magnitude of what DGLs in any community could be asked to do is quite extensive for one person. They could be asked to protect against misuse or improper processing of data by either government, rogue actors, or private enterprises; they could be asked to evaluate a situation in which one was concerned that a senior citizen's lack of technological decision-making capacity was

being exploited; they could be responsible for promoting digital well-being or special protections for minors on the internet. Any one of these tasks is a significant undertaking worthy of the efforts of an entire committee. Much of this might have to be referred up to a DPA, if one exists. The presence of strong central government, extensive technological literacy, and sustained outcry about a lack of digital protections will speed the adoption of these enforcement bodies. Where any one of these variables is lacking, it will be more challenging to assemble the resources to establish a DGL system.

C. Threats Posed by International Actors in Africa's Digital Space

1. The West

Given that Europe, through extraterritoriality requirements, has insisted that international players abide by their data protection standards, it is worth asking whether European companies abide by the same standards when handling the personal data of Africans as they do when handling that of Europeans. A study by Internet Sans Frontières, a digital rights advocacy group, revealed that the subsidiaries of European telecom companies Orange and Vodafone located in Senegal and Kenya granted Africans fewer digital rights than their European subscribers.[116] This was evidenced by a failure to publish the terms of use for their prepaid services, minimal details on the nature of data they collected, the third parties who had access to it, and the security measures they implemented to protect that data.[117] This illustrates that despite the values that animate the European data protection regime, companies will try to cut corners and exploit regulatory weaknesses in countries to the extent they can.

---

[116] INTERNET SANS FRONTIÈRES, DIGITAL RIGHTS IN SUB SAHARAN AFRICA: ANALYSIS OF PRACTICES BY ORANGE IN SENEGAL AND SAFARICOM IN KENYA 27-28 (Jan. 2018), https://perma.cc/E3AV-X5Y3.
[117] *Id.* at 12, 15, 21-22.

U.S. companies have been notorious for neglecting user data privacy considerations, offering convenience added by their products or services in exchange for staggering quantities of personal data. This practice has been perpetuated by the fact that markets do not currently exist for people to understand the value of personal data concerning them, and as such, they are often willing to trade this data for very little. This is illustrated in the case of Branch, a San Francisco-based microlending app currently operating in Kenya and Nigeria.[118] As of 2018, Branch had secured millions of dollars in U.S. venture capital funding to give out loans ranging from 2 to 1000 USD to individuals in areas where credit is rare or inaccessible.[119] The company creates a system of simulated credit to determine whether or not an applicant is eligible for a loan populated by information such as handset details keystrokes and other patterns of app usage), SMS logs, repayment history to the extent available, GPS data, call logs, and contact lists.[120] Users are expected to exchange these data points for access to capital—meaning that Branch's profit scheme is based on the willingness of individuals in vulnerable socioeconomic conditions to trade some of their most telling data points for as little as 2 USD.

While these funds may suffice to cover necessary expenses and bridge people's immediate circumstances, there is a strong argument to be made that the business model underlying Branch is fundamentally exploitative. In 2017, the company's website disingenuously conveyed information regarding data privacy; in the "Commitment to Privacy and Security" section, Branch stated, "We encrypt the data you choose to share with us to protect your privacy. We do not share your information with third parties."[121] However, the privacy policy at that time explicitly stated that Branch may disclose user data to third parties under certain circumstances, stating among other things, "We may disclose some or all

---

[118] *How It Works*, BRANCH, https://perma.cc/5J3M-QPNY.
[119] Connie Loizos, *This Young Lending Startup Just Secured $70 Million to Lend $2 at a Time*, TECHCRUNCH (Mar. 28, 2018, 7:00 AM PDT), https://perma.cc/QR2V-MJ7N.
[120] BRANCH, *supra* note 118.
[121] *Privacy Policy*, BRANCH, https://perma.cc/8DDG-L4UR.

of the data we collect from you when you download or use the App to credit reference bureaus."[122] The website has since been updated to read "[w]e never sell customer data or share customer contacts with third parties."[123] This scenario raises questions about savvy international companies who may enter African countries to take advantage of the nexus of growing technological capabilities, consumers with increasing purchasing power, and weak enforcement of data privacy protections.

2. China

Chinese involvement in Africa has been crucial to the development seen on the continent in the last two decades, and bilateral relations between China and African countries continue to deepen. The nature of Chinese economic engagement with Africa has largely been characterized by infrastructure and construction projects, "such as major railways, including the Standard Gauge Railway in Kenya and the electric railway connecting Djibouti and Ethiopia."[124] In 2013, the Belt and Road Initiative (BRI), an international development plan spanning seventy countries and estimated to cost as much as $8 trillion, was announced, and several of these projects are underway in Central Asia and Africa.[125] Since 2018 however, Chinese government officials have started speaking about a virtual dimension to the BRI: a "Digital Silk Road."[126] While it is unclear what all might be encompassed by the Digital Silk Road, it is clear that it "represents China's vision of global internet expansion via improved telecom infrastructure, the promotion of internet services, cross border e-

[122] *Id.*

[123] BRANCH, *supra* note 118.

[124] Adrian Garcia, *China Embarks on Digital Silk Road*, INVESCO (May 27, 2019), https://perma.cc/S7Q6-3ZAN.

[125] Jonathan Hillman, *How Big Is China's Belt and Road*?, CTR. STRATEGIC & INT'L STUD. (Apr. 3, 2018), https://perma.cc/7ETF-HP2M.

[126] *China Talks of Building a "Digital Silk Road*," ECONOMIST (May 31, 2018), https://perma.cc/C4HT-YTLC.

commerce and trade."[127] President Xi has expressed that "quantum computing, nanotechnology, artificial intelligence, big data, and cloud storage," will be components.[128] He has also stated that "the digital Silk Road [will] involve helping other countries to build digital infrastructure and develop internet security . . . . [And] help to create a community of common destiny in cyberspace."[129] One of the most recent projects launched under this initiative is "the development of a 150,000 kilometer optical cable network, international trunk passageways, mobile structures and e-commerce links designed to build an African 'information highway.'"[130] Almost fifty similar projects are being considered, and the total amount of investment is expected to exceed $70 billion.[131]

For African countries looking to develop and modernize their telecommunications and technology sectors, China presents the most viable and compelling opportunities for partnership. Even before BRI, Chinese companies had invested billions into the continent and have been making relationships and inroads for many years.[132] Most of Africa's telecommunications infrastructure has been built by Chinese telecom giants Huawei and ZTE, and in July 2020, Huawei became the first provider to bring 5G to the African continent through a partnership with a South African network operator, Rain.[133] In 2019, Huawei held trials for preliminary launches of 5G with MTN, Vodacom and Safaricom—Africa's largest telecommunications providers.[134] As of March 2021, the Vodacom and MTN

---

[127] Garcia, *supra* note 124.
[128] ECONOMIST, *supra* note 126.
[129] *Id.*
[130] Garcia, *supra* note 124.
[131] *Id.*
[132] Alicia García-Herrero & Jianwei Xu, *China's Investment in Africa: What the Data Really Says, and the Implications for Europe*, BRUEGEL (July 22, 2019), https://perma.cc/GQ3X-QKYK.
[133] *Rain and Huawei Jointly Launch Africa's First Standalone 5G Network*, HUAWEI (July 19, 2020), https://perma.cc/YF89-GPWU.
[134] Emeka Umejei, *Huawei's Threat to Democratisation in Africa*, E. ASIA F. (Apr. 15, 2019), https://perma.cc/87ZM-KTC2.

networks are operational,[135] but Safaricom decided to suspend the deployment of the 5G network for undisclosed reasons.[136] In the absence of viable alternatives for ICT development, it is difficult to conceive of an Africa in which Chinese ICT infrastructure is not pervasive.

Partnering with China on these large-scale projects comes with certain conditions that pose risks on a variety of fronts. One common concern raised both by outsiders and countries that have partnered with China on previous infrastructure projects is that the deal terms are skewed toward China, saddle countries with debt over a long period of time, and leave these countries responsible for the costs even when the projects are deficient.[137] When it comes to digital infrastructure, the risk of technical failure pales in comparison to the risks to national security and the data privacy of individuals. In 2020, Freedom House's annual Freedom on the Net report ranked China as the "world's worst abuser of internet freedom for the sixth consecutive year."[138] For investments in the Digital Silk Road, China has required the exclusive use of Chinese suppliers, who could facilitate the transport of vast amounts of personal, government, and financial data back to the mainland to be shared with the Chinese government.[139] These concerns cannot be overstated. China's 2017 National Intelligence Law requires "private companies with headquarters in China to cooperate with intelligence services,"[140] and Chinese

---

[135] Yomi Kazeem, *The 5G "Revolution" Is Underway in Africa—but It Remains a Long Way off from Reality*, QUARTZ AFR. (Oct. 2, 2020), https://perma.cc/9ABQ-CGUK.

[136] Eric Olander, *Kenya's Safaricom to Suspend Huawei 5G Mobile Network*, AFR. REP. (Jan. 6, 2021, 1:55 PM), https://perma.cc/39UM-RJU2.

[137] *See* Howard W. French, *The Next Empire*, ATLANTIC (May 2010), https://perma.cc/HB5H-HM7K ("The railroad—known as the Tazara line—was built by China in the early 1970s, at a cost of nearly $500 million. . . . At the time of its construction, it was the third-largest infrastructure project ever undertaken in Africa, after the Aswan Dam in Egypt and the Volta Dam in Ghana. Today the Tazara is a talisman of faded hopes and failed economic schemes. . . . Maintenance costs have saddled Tanzania and Zambia with debts reportedly as high as $700 million in total, and the line now has only about 300 of the 2,000 wagons it needs to function normally.").

[138] FREEDOM HOUSE, FREEDOM ON THE NET 2020 COUNTRY REPORT: CHINA, https://perma.cc/L4H6-T9QH (last visited Apr. 18, 2021).

[139] Garcia, *supra* note 124.

[140] Umejei, *supra* note 134.

state-owned enterprises (SOEs) working with local entities in Africa may be subject to greater demands for information. Chinese businesspeople such as Huawei executive Wang Weijing have been arrested for espionage and related activities in the European Union.[141]

Ample signs suggest that Chinese surveillance on the African continent is already pervasive. In 2018, the French newspaper *Le Monde* published an investigation alleging that China had spied on the servers at the African Union (AU) headquarters in Addis Ababa from 2012 to 2017 and gained access to extensive confidential information.[142] The 200 million USD required for the building came from Chinese state funding, and it was constructed by a Chinese SOE.[143] This SOE was also responsible for providing and installing the computer network, in which a backdoor was allegedly built in that allowed for the data transfers.[144] The hack went undetected for five years until January 2017, when technicians noticed that a peak in data usage was occurring between midnight and 2 AM despite the fact that the building was empty.[145] After investigating, it was found that the AU's confidential data was being transmitted and copied on to servers in Shanghai.[146] News of the event remained secret for a year following its discovery.[147] The Chinese government has denied reports relating to this incident, but the AU has since acquired its own servers, encrypted all of its electronic communications, implemented other enhanced security features, and no longer uses Ethiopia's state-run operator Ethio Telecom.[148] Nairobi-based investment analyst Aly-Khan Satchu noted that the AU hack caused alarm "partly because it exposed that African countries have no leverage over China." He added, "[t]here's this

---

[141] *Id.*
[142] Abdi Latif Dahir, *China "Gifted" the African Union a Headquarters Building and Then Allegedly Bugged It for State Secrets*, QUARTZ AFR. (Jan. 30, 2018), https://perma.cc/KL7F-BBRV.
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] John Aglionby et al., *African Union Accuses China of Hacking Headquarters*, FIN. TIMES (Jan. 29, 2018), https://perma.cc/ADW8-UNTP.
[148] *Id.*

theory in Africa that China is Santa Claus. It isn't. Our leaders need to be disavowed of that notion."[149]

Concerns have also been raised over how China may be exporting its norms towards digital ecosystems along with the technology itself, which may contribute to the empowering and entrenchment of authoritarianism in some African countries. In China, the government sees the internet as a component of its sovereign domain, which sharply contrasts with the notion largely held in the West that the internet is a borderless environment.[150] In defense of Chinese cyber sovereignty, President Xi Jinping said, "We should respect the right of individual countries to independently choose their own path of cyber development and model of cyber-regulation and participate in international cyberspace governance on an equal footing."[151] Nonetheless, by embracing the Chinese model, characterized by extensive censorship and automated surveillance systems, Africa's transitional democracies—and those therein fighting for online freedom of expression and political pluralism—would suffer dire consequences.

IV. REGULATING TOWARDS COMPETITIVENESS AND SAFETY IN POST-DIGITAL ECONOMIES

A. Policy Objectives and Priorities

African countries can recognize that Western privacy norms largely govern the global economy within which their businesses must compete while crafting local policies in a way that connects with citizens and is informed by their particular needs. Towards this end, legislation must address:

- **Proper use.** This encompasses requirements governing collection, purpose specification, storage, and transfer of

[149] *Id.*
[150] Shannon Tiezzi, *China's 'Sovereign Internet'*, DIPLOMAT (June 24, 2014), https://perma.cc/D628-CD86.
[151] Umejei, *supra* note 134.

personal data. While the GDPR and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data may provide some direction, neither can be said to truly represent a "global consensus on the basic principles of how and when data can be collected and disclosed" when virtually no non-Western countries were present when these consensuses were reached.[152]

- **Security.** Data breaches will inevitably affect end users' trust in the data controller, be it a public or private sector entity. Nonetheless, having a protocol in the instance of a data breach, using proper tools and strategies to prevent breaches, and having government policy that increases the incentives to avoid breaches will go a long way in ensuring that such catastrophic events happen as rarely as possible with the lowest possible cost.[153]

- **Public-Sector Protocols**. While new tools are useful in assisting the legitimate functions of law enforcement, policy frameworks need to establish clear and well-conceived boundaries between governments and citizens when it comes to the acquisition and processing of personal data, especially in certain countries where surveillance overreach and public-sector mismanagement of personal data has repeatedly occurred.[154]

- **Identity**. Many African countries without identity systems have leapfrogged into new digital technologies which will allow them to develop state-of-the-art systems fairly quickly and help individuals who lack proof of

[152] MICHAEL KENDE, PROMOTING THE AFRICAN INTERNET ECONOMY (Internet Soc'y eds., Nov. 2017), https://perma.cc/6GRL-247R.
[153] *Id.*
[154] *Id.*

> identity access a number of services such as healthcare, education, and financial services.[155] However, laws must govern the data used to populate new digital identity systems—particularly sensitive and biometric data.[156]

Governments can tailor policies to achieve these goals, but DPAs will determine how they are implemented and whether the policies serve their proper functions. DPAs should assume responsibility for guaranteeing legal certainty through consistent enforcement. They should also provide expert input to their respective governments on how laws may be insufficient or otherwise ill-equipped to achieve their intended purposes. They should investigate alleged privacy violations, impose sanctions where applicable, and work alongside data controllers and other stakeholder groups, communicating with them to offer and receive guidance.

B. Structural Guidance to Align Corporate Incentives

Establishing a framework for respecting human rights regarding technology can set expectations for corporations and public sector entities handling personal data. These frameworks can also provide benchmarks for those seeking to be more responsible with the digital assets of their customers and constituents. The UN Guiding Principles on Business and Human Rights (UNGPs) are worth considering as a model for addressing these issues worldwide, but particularly in Africa, as they are meant to be implemented with, "particular attention to the rights and needs of, as well as the challenges faced by, individuals from groups or populations that may be at heightened risk of becoming vulnerable or

---

[155] Finnbarr Toesland, *African Countries Embracing Biometrics, Digital IDs*, UNITED NATIONS AFR. RENEWAL (Feb. 5, 2021), https://perma.cc/79UC-9QD3.
[156] *Id.*

marginalized."[157] Among the components of the UNGPs that speak directly to the major challenges faced by Africans are two processes contained within the principles. The first is a process of human rights due diligence, which is essentially an audit to identify, prevent, mitigate, and account for an entity's impacts on human rights.[158] The second is a non-judicial process focused on finding remedies for any adverse human rights impacts caused or contributed to by an entity.[159]

In 2019, The UN Human Rights Office of the High Commissioner launched the B-Tech project, aimed at addressing "the urgent need" voiced by companies, civil society, and policymakers "to find principled and pragmatic ways to prevent and address human rights harms connected with the development of digital technologies and their use by corporate, government, and non-governmental actors, including individual users."[160] The UN Secretary-General's High-Level Panel Report on Digital Cooperation acknowledged that "there is now a critical need for clearer guidance about what should be expected on human rights from private companies as they develop and deploy digital technologies."[161] It was recognized that the UNGPs, given their model and mission, had a role to play in providing guidance in the context of digital technologies. As such, the B-Tech project draws on the UNGPs, and will be based on research in four strategic focus areas, all of which speak not just to the threats posed by digital technologies generally, but specifically those to which Africans are most vulnerable.

Focus Area 1: Addressing Human Rights Risks in Business Models

---

[157] U.N. HUM. RTS. OFF. OF THE HIGH COMM'R, GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS: IMPLEMENTING THE UNITED NATIONS "PROTECT, RESPECT AND REMEDY" FRAMEWORK 1 (2011), https://perma.cc/R54G-4XPA.

[158] *Id.* at 17.

[159] *Id.* at 27.

[160] U.N. HUM. RTS. OFF. OF THE HIGH COMM'R, UN HUMAN RIGHTS BUSINESS AND HUMAN RIGHTS IN TECHNOLOGY PROJECT (B-TECH): APPLYING THE UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS TO DIGITAL TECHNOLOGIES 2-3 (Nov. 2019), https://perma.cc/ZY44-RQSD.

[161] *Id.* at 2.

This focus area seeks to explore and address the risks of business models that could be exploitative to vulnerable populations. Several examples mentioned earlier in this Note employ business models described in this focus area. These are businesses or other entities that as part of their operations involve:

> a) Gathering large volumes of personal data (whether to train algorithms or sell insights to third parties);
>
> b) Selling products to governments seeking to use new technologies for State functions that could disproportionately put vulnerable populations at risk;
>
> c) The promise of hyper-personalization in human resources or marketing decisions which could lead to discrimination;
>
> d) Using "algorithmic bosses" to mediate the relationship between workers and firms that generate business value from the offline work being done, while limiting labor protections for those workers;
>
> e) Providing a technology which allows vast numbers of small and medium enterprises, or individuals to conduct activities that may result in harm to people, but where control over their activities might be limited; and
>
> f) Models that are informed by, or inform, the personal choices and behaviors of populations without their knowledge and consent.[162]

Focus Area 2: Human Rights Due Diligence and End-Use

How human rights due diligence is conceived of in the B-Tech project differs slightly from its conception in the original UNGPs. Rather than just extending to a company's operations, due diligence in this context

---

[162] *Id.* at 5.

encompasses end-use of a company's products and services. As such, the level of action required of companies is greater in this context. The UN suggests that appropriate action includes, among other things, creating leverage over those who either produce or perpetuate the harm, whether they be individuals or entities.[163] This can be achieved within bilateral relationships with customers "by setting norms and expectation of behaviors for users; through establishing industry standards and good practices; or by engaging constructively with regulatory and public policy efforts to prevent harm."[164] While framing due diligence in this way may have its merits, it might create complication surrounding the attribution of responsibility for harms, given that there are many points along the value chain that may contribute to adverse impacts on an end user.

Focus Area 3: Accountability and Remedy

This focus area explores the extent to which the grievance mechanisms outlined in the UNGPs can be applicable in the context of digital technologies. It seeks to anticipate certain hurdles and potentially arrive at more relevant processes by asking challenging questions such as these:

- To what extent are technology companies already using non-judicial grievance mechanisms to address alleged human rights abuses directly linked to their operations, products, services, or business relationships?[165]

- How can companies establish genuinely effective remedy mechanisms if they must prioritize among hundreds of thousands, or even millions, of potentially impacted individuals and human rights issues?[166]

---

[163] *Id.* at 7.
[164] *Id.*
[165] *Id.* at 8.
[166] *Id.*

- In a given geography, might it be necessary for different actors in the technology sector (e.g., ISPs, telecommunications providers, social media platforms, researchers) to establish joint grievance mechanisms, and collaborate on remedies?[167]

- What is the role of state regulation in supporting extrajudicial remedial efforts by technology companies, and how can resolution be achieved in scenarios where conflicting regulations in different jurisdictions pose problems for non-judicial grievance mechanisms?[168]

- What are the responsibilities of corporate providers of digital technologies to provide effective remedies in cases where individuals– versus public or private entities— misuse their products?[169]

Focus Area 4: "A Smart Mix of Measures": Exploring regulatory and policy responses to human rights challenges linked to digital technologies

This focus area deals with policy innovation, recognizing that the incentives of policymakers may not be in line with what best fosters human rights. Some of the research already done in this focus area has shown that "very few national strategies explicitly address human rights or prioritize the safety of AI systems."[170] As artificial intelligence systems have been deployed in several African countries with no regulatory guidance, it can be observed that certain governments are not prioritizing the human rights implications of these technologies. Policies that excessively privilege individual state interests and priorities may create "conflicting regulatory requirements for business and other actors to navigate."[171] The "*Smart Mix of Measures*" described by the B-Tech project draws on

[167] *Id.*
[168] *Id.*
[169] *Id.*
[170] *Id.* at 9.
[171] *Id.*

one of the underlying takeaways from the UNGPs in recognizing that for intricate human rights concerns posed by digital technologies whose impacts cross myriad borders and boundaries, a single level of regulation is insufficient to create a robust and functional ecosystem.[172] Mandatory measures at the state level should work in tandem with voluntary extrajudicial processes, which can also be supported by either mandatory or voluntary international or regional conventions.

C. Coordinating Enforcement on a Multinational Level

African countries must find ways to focus data protection legislation on their unique priorities and enforce violations reliably. Effective cross-border conventions will be crucial for the completion of data protection ecosystems in Africa. While copying European law may not be effective, Africa can learn from the EU in mirroring the way it streamlined its data protection regime and insisted that the rest of the world respect it. When the regulation was issued, there were uncertainties around the EU's extraterritorial enforcement ability, but fines have been issued, and companies across the world have changed their practices to comply.[173] The EU's approach was effective because companies recognized that the potential for significant revenue losses in the EU market would be far more expensive than the costs associated with compliance.

African countries are not bound under a common set of laws at the supranational level like the EU, but stakeholders across borders should be sufficiently and strategically motivated to work together. Population growth in Africa is high, the purchasing power of Africans is increasing, and the costs of missing out on this consumer base will multiply in the years to come, but no single country is positioned to wield this leverage and tilt the cost-benefit analysis for most companies by acting alone.[174]

---

[172] *Id.*

[173] *14 Biggest GDPR Fines of 2020 and 2021 (So Far)*, TESSIAN (Feb. 3, 2021), https://perma.cc/LEK9-CD8Y.

[174] Landry Signé, *Africa's Emerging Economies to Take the Lead in Consumer Market Growth*, BROOKINGS (Apr. 3, 2019), https://perma.cc/9V9V-F2MF.

Working within and across the existing African regional blocs such as the EAC, SADC, and ECOWAS to revisit existing data protection conventions is a natural starting point for serious action. While not a substitute for effective national law, regional and subregional conventions are likely the best vehicles to add teeth and thoughtful contextual adaptations to internet regulations, tailoring to cultural forces.

V. CONCLUSION

The Information Age presents endless possibilities for African countries, but they will not be able to take full advantage of these possibilities by governing the digital space with laws that do not meet their particular contexts, challenges, and circumstances. As global standards form in this arena, African nations should be contributors, not simply adopters. This necessitates a comprehensive understanding of existing frameworks, followed by earnest efforts to improve upon them. While the GDPR may be a landmark piece of legislation, many of its shortcomings in rapidly changing, diverse technological and social environments have been made known. It is critical to recognize that while many aspects of the GDPR are arguably universal, it is a Eurocentric policy that was born out of years of discussions among European stakeholders. It is long past time for African stakeholders to have productive discussions to identify their priorities in internet governance with an eye towards the continent's youth and desired position in the decades to come. There must be a diversity of voices and perspectives at the table so lawmakers can comprehensively understand the needs of various constituencies. There must be honesty and transparency surrounding the relationship between the government and its citizens and clarity surrounding boundaries set in constitutions. Once legislation is ratified, African leaders should see that implementation follows as soon as possible thereafter, and aim to stick to predetermined timelines to create confidence in these laws. Several countries have passed laws without following through on realizing enforcement mechanisms spelled out in the law, such as creating and funding a DPA. Other countries have moved so slowly in rolling out enforcement

provisions that it has created confusion among individuals and businesses trying to plan for a new environment.

National legislation is insufficient to ensure robust data privacy and digital rights protections for citizens, especially in countries and regions where the rule of law is weak. Establishing strong multinational conventions around shared principles and a commitment to fining violators will deter both domestic and foreign actors who seek to take advantage of weak national enforcement. Conversations among stakeholders on the African continent seeking to create these conventions should resume where they have stalled, and countries should revisit, strengthen, and ratify existing multilateral agreements. Governments should take guidance from the UNGPs and collaborate with the private sector in the creation of extrajudicial systems to address digital rights harms.

Civil society groups have a crucial role to play in educating the public about the value of personal data and the tangible threats that exist from both public sector and private sector data collection and processing. Advocates from these organizations can lobby the government, but they should make sure that they are giving guidance on the community level. Community-based enforcement can be effective when trusted stakeholders are part of these initiatives, and when they have the backing of governments. Personal data protection and digital rights are of paramount importance to guarantee the safety of everyday people in a rapidly evolving world. Regulations in Africa must address the realities and needs of Africans and keep pace with innovation if this is to be the case.