Science Discovery Public Health
2026, Vol. 1, No. 2, pp. 50–55
https://doi.org/10.11648/j.sdph.20260102.11

Research Article

Extending Encryption Through Privacy Protection for Healthy Internet in Africa

Abraham Selby*

School of Public Policy, University College London, London, United Kingdom

Abstract

Africa's digital revolution is unfolding at lightning speed, but its success hinges on one fundamental need: protecting people's privacy and personal data. As worries grow about surveillance, cyber threats, and uneven data regulations, encryption emerges as a vital shield for personal information and a cornerstone for building trust online. This paper explores how end-to-end encryption, backed by strong privacy safeguards, can help create a healthier, more resilient internet ecosystem across Africa. We examine the continent's current data privacy landscape, drawing on frameworks like the African Union's Convention on Cybersecurity and Personal Data Protection. The reality reveals significant gaps: weak enforcement, restrictive laws, and infrastructure challenges often block the effective use of encryption to keep people safe. But within these challenges lie clear opportunities for progress. Building a secure digital future isn't a solo effort. This research highlights the essential roles governments, civil society, academics, businesses, and tech experts must play together to champion and implement robust encryption standards. We review key techniques thus protecting data at rest, in transit, and even in use with the focus on their critical importance for securing everyday online activities like shopping, communication, and remote work. Real-world examples from Ghana, South Africa, and Tunisia showcase diverse approaches and their impact on internet health. Ultimately, we make the case for a harmonized regional approach. By fostering true collaboration among all stakeholders, Africa can embed encryption as a foundational element of its digital journey. Prioritizing privacy through encryption isn't just about security; it's about empowering users, enabling inclusive digital economies, and ensuring the internet serves Africa’s people sustainably and fairly.

Keywords

Internet Governance, Data Protection, Encryption, Privacy, Africa, Multistakeholder Regulation, ICT Policy, Digital Transformation

1. Introduction

The Internet has become a way of life in the digital world. Within every minute in an hour, individuals connect online by sharing information and ideas, communicating, and collaborative working tasks. The multi-stakeholder groups within the Internet Governance Ecosystem; Civil Society, Technical Community, Private Sector, Government, Academia, etc. are always working together to extend encryption through the usage of the internet thus protecting the privacy of the internet users through data sharing and information protection. [1].

In strengthening the Internet, The Internet Society states in their action plan advocating for end-to-end encryption, secure global routing, facilitating knowledge exchange about network

*Correspondence: Abraham Selby (Selby.abraham@yahoo.com)

Received: 21 July 2025; **Accepted:** 31 July 2025; **Published:** 28 April 2026

and distributed system security, and examining the many ways digital sovereignty is interpreted by those who seek to assert it. [1].

The report calling for better online data privacy regulations and stakeholder coordination for greater impact comes at the end of a six-month study undertaken by Stears Data, with support from Luminate, a global philanthropic organization focused on empowering people and institutions to work together to build just and fair societies. [2]. The report provided insight into key issues in data and digital rights; effective approaches to addressing those issues; and opportunities for impact, with input from representatives in the public and private sectors, civil society, and media [2]. On data protection, the study found that "there is insufficient judicial and regulatory oversight available to sufficiently protect personal data" as provisions in the telecommunication and cybercrime legislation can be exploited for surveillance purposes by government departments. [2].

However, we can work to see the privacy protection of individuals being regulated well by the various stakeholder groups. This can be a regime through encryption of personal data for healthy internet usage in Africa. As stated in the Internet Society report, the most effective way to ensure the personal security of billions of people and the security of nations around the world is to not only continue preserving uncompromised, end-to-end encryption practices, but also by adopting and bolstering strong encryption policies. [3].

2. Exploring Perspectives on Privacy Protection in Africa

As stated by the IGF theme in data governance and privacy protection, Data is a key resource in the global digital age [4]. In Africa, data protection is always evolving in our everyday digital world and privacy protection is a key component related to data protection. Privacy protection refers to the ability to keep the information you'd like to save to yourself from getting into the hands of companies, hackers, government organizations, and other groups or the public. Also, Organization has a role to keep the personal data of their customers and clients in a secure way that does not go out to unauthorized users which shows that Privacy protection describes the ability to keep specific information private or restricted to a limited number of people. Privacy protection consists of physical protection, virtual protection, third-party protection, and legislation protection for healthy internet and digital engagement. [5].

The African Union Convention on Cybersecurity and Personal Data Protection has been signed by 14 countries, and only eight countries ratified it by June 2020. Indeed, adherence to these instruments remains low [6].

3. The Privacy Protection Implications and Limitations Against Healthy Internet Usage

It is known by a report from Dalberg's advisors that the absence of existing data protection frameworks and the lack of supporting services presents a significant challenge for most African countries. With no African country currently deemed to be compliant with the GDPR, its introduction risks disrupting the USD 14 billion in annual exports from Africa's digital economy to the EU. [7].

These limitations are connected to the various data protection principles below; Firstly, Collecting Data is a limitation to privacy protection. This means that Personal data must not be obtained and processed lawfully, fairly, and, to the extent possible, transparently in Africa. The quality of data is another limitation to privacy protection which shows that personal data sometimes is not accurate at the point of collection, and we must ensure reasonable steps are taken in the accuracy of data and how data is maintained throughout retention. Another limitation or implication is the purpose of specification of data which defines how personal data is collected only for specified, explicit, and legitimate purposes. This ensures that personal data should only be used for such other purposes as are compatible with applicable laws, such as archiving data that is in the public interest, or for scientific research. [8].

4. Understanding the Discourse on Encryption

To get a healthy internet through the privacy protection of an individual, Encryption in Internet security and privacy protection can be defined as the conversion of data into a readable format into an encoded format with the same data. It is known that encrypted data can only be read or processed after it has been decrypted. In the view of Internet and data protection encryption is set to be the basic building block of data security and data protection for a healthy Internet. In other views, Internet Society defines encryption as the process of scrambling or enciphering data so it can be read only by someone with the means to return it to its original state which also states that there is a crucial feature of a safe and trustworthy Internet. It helps provide data security for sensitive information. [3].

From the report of CEPA, it is shown that encryption concerns in Africa include prohibitive regulation that hampers the use of encryption, compelled assistance by service providers, mandatory SIM card registration, and data localization requirements. All these can be exploited especially by states and their agencies to undermine citizens' right to privacy and various other digital rights [9]. CEPA reports also show that encryption is under threat from governments in Africa, as in other parts of the world. Among the concerns cited by the brief are legislation and regulations that require registration and licensing of encryption service providers before they can offer

cryptographic services.

This is the case in Benin, Chad, Cameroon, Congo Brazzaville, Democratic Republic of Congo (DR Congo), Ethiopia, Guinea, Ivory Coast, Malawi, Mali, Morocco, Senegal, South Africa, Tanzania, Tunisia, and Zambia, among others. Offering encryption services without a license attracts penalties, as does failure to hand over secret encryption codes to state authorities, or using prohibited encryption tools. [10].

5. Some Various Modes Where Encryption Is Needed for Privacy Protection

With respect to Online business and Electronic Commerce, the use of encryption is needed to protect the privacy of user data on the internet. There is a trusted business to protect our financial transaction information when we buy and sell things online or when we use internet banking and other payment solutions. Encryption is then a key method in performing such a transaction.

Browsing is another mode in which encryption is needed to protect the privacy of the user and their data. This ensures that browsers and websites use HTTPS and an encrypted protocol, to provide secure communications, keeping our data from being read by bad actors while in transit use of the internet.

In secure messaging, encryption plays a key role, and this is when we use a messaging app, we expect the messages to be private. Some messaging apps use encryption to maintain the privacy and security of their users' communications while it is in transit. Others even use end-to-end encryption, so only the sender and receiver can read the messages. An example is the WhatsApp feature that uses end-to-end- encryption method to protect the information or communication from one user to another.

6. The Need to Increase Encryption to Protect Privacy

Some of the raised facts in Africa concerning encryption are prohibitive regulation that hampers the use of encryption, compelled assistance by service providers, mandatory SIM card registration, and data localization requirements. All these can be exploited especially by states and their agencies to undermine citizens' right to privacy and various other digital rights. In Ghana from July 2021 to date, the government in partnership with the ministry of communication and the National Communication Authority has set policies and regulations to enroll on a mass sim card re-registration with the citizen identity Card (National ID). This is to ensure that the security and protection of individuals are protected by service providers. [11].

Some of the key benefits of using encryption are to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network. Also, encryption Increases consumer trust in privacy protection. Although entities in Africa will not have strict regulatory encryption requirement while companies may wish to use encryption to gain trust from their customers. From CIGI-Ipsos Global Survey on Internet Security and Trust, "53% of respondents said they were more concerned about online privacy now than a year ago". Given the erosion of trust that we've seen in recent years, advertising the fact that your business is conforming to certain encryption standards could give you a competitive advantage. [12]. looking at the rate at which the pandemic forced all entities to adopt remote working, encryption helps in Protecting Remote Workers. It is believed that the risk of a data breach is higher when employees work remotely. This is not surprising as many remote workers store confidential data on their devices, and companies have little control over how this data is accessed and shared. If companies enforce strict encryption, remote workers' privacy will be protected while using the internet for healthy workplace. [12].

7. Some Means and Approaches in Which Encryption Can Be Used to Protect Privacy in Africa

Firstly, we can use encryption at rest as a way to protect the privacy of individuals in Africa. This means Encrypted data stored in servers and/or in databases. In the case of data exfiltration, or if the network/systems are compromised, the data will remain encrypted. Examples are the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) [13].

Secondly, Encryption-in-transit is a means by which the privacy of data can be protected, and this Encrypts traffic between two entities or systems which also protects against MITM or sniffing, where even if communication is intercepted, it becomes useless. Encryption is done at the transport layer. Upon receiving the message, the endpoint is authenticated, then data is decrypted and verified. Examples are TLS or Transport Layer Security which is often used for encryption in transit. [13].

Thirdly, Encryption-in-use is also another way to protect the privacy of the individual which seeks to Protect the data while it is being used to run analytics or computation lining it with an example of Format Preserving Encryption (FPE). [13].

Looking further at the above means we can say that the various stakeholder groups must ensure or use these strategies stated below for effective encryption of data for a healthy internet in Africa.

One is the Classification of data: At the beginning, Companies or stakeholders need to identify what data to encrypt. We must understand and classify the different types of data being transmitted and stored (e.g., credit card numbers, customer information, company proprietary data) which is based on sensitivity, use, and regulatory impact. [14].

Another strategy is to Implement a strong key management practice. This is when keys fall into the wrong hands, where organizational data security is at stake. Policymakers need to keep an inventory of all the encryption keys, along with information on who has access to them and how and when the keys have been used. Key management solutions help you to store and manage encryption keys. This can also be done through inter-governmental capacity-building training and awareness training that can be enforced on various companies to follow as far as data protection and privacy of the citizens are concerned. [15].

8. The Role of Multistakeholder Groups in Strengthening the Internet Through Encryption and Privacy Protection

From learning resources in Introduction of internet governance by Internet Society, the Internet governance multistakeholder group model plays a key role in policies when it comes to the internet and digital protection. The multistakeholder model of Internet governance is also known as the best mechanism for maintaining an open, resilient, and secure Internet because, among other things, this is informed by a broad foundation of interested parties which includes businesses, technical community, civil society, academia, governments, and IGO's with a common goal.

It is recommended that the Government stakeholder group has to set policies and regulations that can protect various individuals' privacy in their respective countries through a compliance model. The Technical Community must also ensure that there is system security, data encryption, access control mechanisms, database protection, network security, and other aspects of protecting the privacy of individuals and the internet. Academia as a multistakeholder group should be able to create training awareness and skills training for its community which will enable individuals able to know how to protect their privacy through encryption for a healthy internet. The private and business stakeholder group also ensures that institutions provide a common and shared understanding and principles that can guide them to be compliant with the privacy regulations set out by the regulatory authorities. Civil society is concerned about the various communities, the Lay people who need to understand such protection. Civil society must ensure that through local organizations their members understand the key principles and regulations that can help them protect their internet through encryption and protect their privacy for a healthy internet.

9. Conclusion

As reported by Cynthia Rich (2016) Privacy Laws in Africa and the Near East (16) 6 Bloomberg BNA World Data Protection Report, there are currently 17 countries in Africa that have enacted comprehensive personal data protection legislation, namely Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Mali, Mauritius, Morocco, Senegal, Seychelles, South Africa, Tunisia and Western Sahara [16].

Africa Union must be able to sign all African countries for common regulations and privacy impact as we continue to create internet for everyone, growing the internet and also strengthening the internet, the security and privacy is also a key role all multistakeholder groups have to ensure that the internet is healthy for public use. As part of my speech at various conferences and awareness under the Internet Governance Forums and Internet safety, I have personally highlighted the need for data protection in various African countries. I also highlighted the gaps in privacy protection in our various policy regulations in Africa and how the youth can be involved [17]. At the global IGF 2022 where I am speaking about the data privacy gap from the global youth perspective, I recommend that action of awareness to protect privacy for a better and healthy internet among the youth is achieved by all Government stakeholders, Academia, Technical Community, Private Sector, Civil Society and the rest. [18].

In concluding this paper with all the learning from the Internet Society and other groups training, The African Union must be able to come up together policymakers in the various countries with other multistakeholder actors like ICANN, ITU, APC, African IGF, Internet Society to set up a Regional Data Protection regulation Agency and policies like the European Union (GDPR) which can ensure the privacy protection in Africa and also believe that encryption can be used as a tool to protect the privacy of the individual in Africa for a healthy Internet through regulations and policy documentation and implementation through a regional level approach which can help strengthen the internet making everyone connected and safe.

Abbreviations

AU	African Union
AES	Advanced Encryption Standard
FPE	Format Preserving Encryption
DES	Data Encryption Standard
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol Secure
ISOC	Internet Society
IGF	Internet Governance Forum
IGO	International Governmental Organization
ITU	International Telecommunication Union
MITM	Man-In-the-Middle (Attack)
SIM	Subscriber Identity Module
TLS	Transport Layer Security

Acknowledgments

The author extends sincere gratitude to the Internet Society Youth IGF Program for its continued support in building youth

capacity on internet governance and digital rights. Appreciation is also given to the Internet Society Global for providing valuable resources and advocacy on encryption and secure internet practices. Their collective efforts have significantly contributed to shaping this research.

Author Contributions

Abraham Selby: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Software, Validation, Writing – original draft, Writing – review & editing

Funding

This work is not supported by any external funding.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] A Healthy Internet for Future Generation – Internet Society Action Plan 2022, Retrieved From https://www.internetsociety.org/action-plan/2022/

[2] Report sees need to strengthen Internet freedom, data privacy laws, The Guardian, Retrieved From https://guardian.ng/technology/report-sees-need-to-strengthen-internet-freedom-data-privacy-laws/

[3] What is Encryption, Internet Society, Retrieved From https://www.internetsociety.org/issues/encryption/what-is/

[4] IGF 2022 Themes: Descriptions, Governing Data and Protecting Privacy by Internet Governance Forum, Retrieved From https://www.intgovforum.org/en/content/igf-2022-themes-descriptions

[5] Different Types of Privacy Protection, Carol Francois, August 2022. Retrieved From https://www.easytechjunkie.com/what-are-the-different-types-of-privacy-protection.htm

[6] African Union Convention on Cyber Security and Personal Data Protection, African Union, May 2020. Retrieved From https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[7] GDPR: The implications for Africa, Dalberg Advisors, May 2018, Retrieved From https://dalberg.com/our-ideas/gdpr-implications-africa/

[8] Personal Data Protection Guidelines for Africa, A joint initiative of the Internet Society and the Commission of the African Union, May 2018, Retrieved From https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

[9] How African Governments Undermine the Use of Encryption, CEPA October 2021, Retrieved From https://cipesa.org/?wpfb_dl=477

[10] Policy Brief: How African States Are Undermining the Use of Encryption, Lillian Nalwoga, October 2021, Retrieved From https://cipesa.org/2021/10/policy-brief-how-african-states-are-undermining-the-use-of-encryption/

[11] Ghana SIM Registration 2021, National Communication Authority, Retrieved From https://nca.org.gh/key-concern-areas-frequently-asked-questions-for-sim-registration-2021/

[12] CIGI-Ipsos Global Survey on Internet Security and Trust, Centre for International Governance Innovation, Retrieved From https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/

[13] How encryption can be used to protect data throughout its lifecycle (data-at-rest, data-in-transit, data-in-use) Retrieved From https://www.encryptionconsulting.com/education-center/encryption-of-data-states/

[14] Benefits of Using Encryption Technology for Data Protection, Brian Jefferson, June 2021. Retrieved From https://www.lepide.com/blog/5-benefits-of-using-encryption-technology-for-data-protection/

[15] Encryption Methods to Shield Sensitive Data From Prying Eyes, Zach Capers, July 2021, Retrieved From https://www.getapp.com/resources/common-encryption-methods/

[16] Privacy & Personal Data Protection Guidelines for Africa, Verengai Mabika, Retrieved From https://www.itu.int/en/ITU-D/Capacity

[17] The state of personal data protection in Africa: a comparative approach, A. Selby, R. Nyarko, B. Manga, S Levy, June 2022, Retrieved From https://rightscon.summit.tc/t/2022/events/the-state-of-personal-data-protection-in-africa-a-comparative-approach-fR13yPTQ8Hd71jinVefHnk

[18] Data Privacy Gap, the global youth Perspective, A. Selby IGF 2022 session. Retrieved From https://www.intgovforum.org/en/content/igf-2022-ws-269-data-privacy-gap-the-global-south-youth-perspective

Biography

Abraham Selby is an Information Technology Consultant, Researcher, Internet Governance Advocate, and Tech Policy Analyst with a strong focus on digital rights and data protection in Africa. He holds a Master's degree in Public Administration and Management and has academic experience from University College London (UCL) in UK. Selby has served as a Technical Support Volunteer for the United Nations Internet Governance Forum (UN IGF) and is actively involved with the Internet Society Global and Youth IGF programs. He has been a mentor for the Internet Society Fellowship Programs since 2023 and a research contributor to the IS3C Skills Gap project. His work centers on digital policy development, multistakeholder internet governance, and building privacy and encryption awareness across African communities. Selby is also the Co-founder of Selby Foundation Network, promoting digital inclusion, youth engagement, and community-based ICT training.

Research Field

Abraham Selby: Digital governance and policy, Internet security and privacy, Data protection frameworks in Africa, Information technology and society, Cybersecurity awareness and training, Multistakeholder internet governance, Sustainable digital development, Youth engagement in technology policy, online human rights advocacy, Digital inclusion and accessibility