Cross-Cultural Perspectives on eHealth Privacy in Africa

Moses Namara
School of Computing
Clemson University
USA
mosesn@clemson.edu

Daricia Wilkinson
School of Computing
Clemson University
USA
dariciaw@clemson.edu

Byron M. Lowens
School of Computing
Clemson University
USA
blowens@clemson.edu

Bart P. Knijnenburg
School of Computing
Clemson University
USA
bartk@clemson.edu

Rita Orji
Department of Computer Science
Dalhousie University
Canada
rita.orji@dal.ca

Remy L. Sekou
IBM Research
Nairobi
Kenya
Sekou.Lionel.Remy@ke.ibm.com

ABSTRACT

The African continent is making considerable strides to develop and implement technology-driven health innovations. Policymakers are increasingly acknowledging the rising concerns for online personal privacy and data protection as advances in eHealth results in increased levels of data collection and surveillance. In this paper, we propose a research agenda to investigate the effect of cultural, constitutional, and societal factors on privacy concerns and preferences among the different African countries in the context of healthcare technologies. In addition to helping us understand policy and design implications for members of this region, this research will broaden our understanding of cultural factors influencing privacy worldwide.

CCS CONCEPTS

• K.4.1 Public Policy Issues → Privacy; *Regulation, Trans-border, data flow* • K.4.4 Electronic Commerce → Security • J.1 Administrative Data Processing → Government, Law

KEYWORDS

Africa, privacy, eHealth, cross-cultural privacy

ACM Reference format:

Moses Namara, Daricia Wilkinson, Byron M. Lowens, Bart P. Knijnenburg, Rita Orji and Remy L. Sekou. 2018. Cross-Cultural Perspectives on eHealth Privacy in Africa. In *Proceedings of ACM 2nd African Conference for Human Computer Interaction (AfriCHI'18). Windhoek, Namibia.* https://doi.org/10.1145/3283458.3283472

AfriCHI'18, December 3-7, 2018, Windhoek, Namibia
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6558-1/18/12$15.00
https://doi.org/10.1145/3283458.3283472

1 INTRODUCTION

Across African countries, increased smartphone penetration and upgraded telecommunication infrastructure coupled with lower connection costs have increased user access and subscription to the Internet [5,12,58,75]. Given this access, users are now able to go beyond standard voice and messaging services and utilize various mobile applications, most predominantly social networking applications such as Facebook Messenger, WhatsApp, Line, Instagram and Snapchat [21]. As a result, social networking sites and messaging applications have become more central in users' daily interaction not only with family and friends but also with health professionals [34]. This has led to creative online health networking (referred to as eHealth) innovations that improve the general welfare and livelihoods of Africans [6,15]. eHealth can be best described as "the use of social software to promote collaboration between patients, their caregivers, medical professionals, and other stakeholders in health through the reliance and use of technology e.g. smartphones " [62].

While eHealth innovations are critical for the provision of healthcare services across African countries, they can also create significant risks to users' online privacy considering that information shared in eHealth applications includes some of the most intimate and sensitive details about someone's life. Beyond mere embarrassment, privacy breaches can also inflict great harm with direct consequences to employment, insurance coverage, and physical safety [47].

In light of this, several African countries acknowledge the need to protect their citizens' (health) information privacy from a legal perspective. However, only a few countries such as Ghana, Mauritius, Morocco, South Africa, and Tunisia have so far developed comprehensive legal frameworks that also have meaningful enforcement policies. At the same time, little is known about the level of awareness of privacy policies in the populace across the continent [20].

Thus, the major purpose of this paper is to propose a pan-African research agenda that is considerate of cultural, constitutional and societal factors to study and eventually shape the continent's perspectives on eHealth privacy for proper privacy protections and management across the continent. The African continent cannot be viewed as a homogenous mass given that regulatory and legislative frameworks differ from country to country. Instead, practical considerations such as regional customs and culture are valuable in understanding how privacy is defined and how that shapes privacy preferences and behaviors compared to adopting a "one-size fits all" approach [52].

In this paper, we adopt this prepossession and take the first step in investigating a cross-cultural privacy behavior and policy analysis for the African continent. In doing so, we analyzed existing regulatory and legislative frameworks and provide recommendations that respect cultural norms and identify the practical design implications.

The paper is structured as follows: section 2 presents the related work covering existing research on internet and social media use for health purposes in Africa, privacy practices and laws in Africa, and practical eHealth use cases. In section 3, we outline our proposed research agenda. In section 4 and 5, from prior knowledge and related work(s), we explain the legal and design implications. Finally, in section 6 we detail our limitations and discuss future work followed by the conclusion in section 7.

2 LITERATURE REVIEW

This section covers existing research on the use of social media for health purposes in Africa, privacy laws and practices in Africa, and case studies of eHealth technologies and their privacy implications.

Africans increasingly use online resources for health purposes. For example, Abebe et al. [1] analyzed health searches related to HIV/AIDs, malaria and tuberculosis made using the Bing search engine from all the 54 African nations. They affirmed the wide-spread interest in various types of information that include disease symptoms, drugs, concerns about breastfeeding, as well as stigma and a belief in natural cures.

In recent years, these practices have switched to social media platforms, and many other eHealth solutions which leverage social media technologies. For example, instant messaging on WhatsApp and Messenger is used as a tool to create support groups, share information, and connect with patients in remote areas. This is important particularly in political situations and insurgencies such as that in Somalia which has made certain populations difficult to reach due to the insecurity in the areas where they reside. Online health networking tools are also used to quickly disseminate information among team members in hospitals, or during epidemic and emergency situations [30]. Compared to face-to-face outreach, the social support that springs from social media platforms helps vulnerable populations and high-risk groups such as HIV infected persons overcome stigma and discrimination [68]. These campaigns and communications on social media can also be tailored to the different languages that are spoken across African populations [24]. Additionally, ehealth applications have been enhanced by the incorporation of mobile financial services [39,43] which are used to easily pay for medical expenses [52].

2.1 The use of Social Media for Health Purposes in Africa

Apart from connecting and communicating with family and friends, social media is used to garner knowledge on critical issues such as health due to the patient's social network that has been shown to have an influence on health-related advice, decisions, and support [25]. Social network technologies are also transforming the way physicians communicate with different stakeholders [27,61]. These effects are emphasized by social media-based health innovations that provide a platform to disseminate much-needed information on disease screening, diagnosis, and treatment, as well as an avenue to conduct health promotions, share experiences, provide social support and promote adherence to medication complementary to physical face-to-face interactions [24,72]. Indeed, a growing number of African populations have adopted and continue to use social media platforms with 67.3% of the population using Facebook at the time of writing [66].

As an example, new mothers form groups on Facebook Messenger and WhatsApp to get post-natal care and information such as how to feed and clean the newborn baby to reduce the risk of disease and infection at a tender age. They usually form and join these groups during the pregnancy period, mostly for antenatal care and education on pregnancy. These groups also give mothers including those in rural areas access to a doctor, who might otherwise be long distances away from them [26]. Via these social media groups, doctors are also able to advise expecting mothers on the importance of observing good health habits (e.g. no smoking or drinking alcohol during pregnancy) and provide special care for expectant mothers with pre-existing conditions such as diabetes and hypertension. For instance, Medici is an instant messaging service in South Africa modelled off WhatsApp which allows patients to contact their doctors via text or video call [10]. Doctors in turn, cater to a more substantial number of patients by responding to their requests without seeing them face-to-face, Moreover, they can limit hospital visits to severe and or complex health matters only, thereby reducing pressure on the hospital system—e.g. in Nairobi, 70% of all hospital visits do not actually require a visit, but without access to other reliable health information, people have nowhere else to turn [77].

A typical health-related social media interaction starts with a user contacting the eHealth app or doctor via the app by describing the problem or asking a question. The eHealth app or doctor subsequently acknowledges the request, resulting in one of several responses [77]:

1. The eHealth app or doctor asks for more details, such as photos that show the problem.
2. The eHealth app or doctor recommends a course of action or treatment.

3. The eHealth app transfers the user to a real doctor who can further assist, or the doctor recommends the user to visit the nearest hospital/clinic.
4. The eHealth app or doctor immediately refers the user to a hospital.

It is clear that in this process, users may have to share sensitive information with doctors (e.g., an HIV/Aids diagnosis). The social media platforms used for these communications are uniquely positioned to share this information with third-party organizations who want to know and learn about it. In some cases, such partnerships have a humanitarian hallmark (e.g., collecting up-to-date information about health epidemics), but they can also serve as one of the revenue streams for the social media application (e.g., selling personal information to health insurers or drug companies).

Such sharing is not without controversy: for example, Townsend [71] found that patients in Africa are reluctant to use eHealth applications and social media platforms if they do not provide proper systems of privacy and data protection. Therefore, care must be taken to ensure that sensitive data is not exposed to third parties.

In summary, while the use of social media in Africa is integral to citizens getting adequate healthcare [35,47], privacy issues may thwart these benefits. Hence, the next subsections discuss privacy practices and laws across the African continent.

2.2 Privacy Practices in Africa

We start this review with an explicit acknowledgment that African privacy values may not always align with western privacy values. For example, it is often assumed that "individual privacy," where an individual can advance claims for privacy, is a less critical value in the non-western world than in the western world. Indeed, while this assumption lacks empirical evidence, group interests are primarily believed to outweigh individual interests in Africa, due to the strong culture of collectivism that exists in African societies [41]. However, most social media platforms such as Facebook store African user data on servers located outside the continent. Under this arrangement, data and privacy protections are subjected to the American or European law, which may not be suited to the African context.

Moreover, even within the Africa context, there exists a significant diversity of practices, concerns, and approaches to privacy [16,18]. These vary according to traditional demographic divides such as urban and rural populations, young and old, women and men [77]. For example, the volume, range, and nature of personal data younger users post on social media sites reflect a sense of ignorance regarding the effect their actions have on the privacy and security of both their own data and that of others [14]. Indeed, Tedre and Chachage [69] in a survey study of Tanzanian university students' attitudes towards e-security issues, found them to harbor lax attitudes towards their password security. In particular, students frequently gave their usernames and passwords not only to other students within the university but to others outside the university, as they felt that one could not do something bad with another's password i.e. "*They feel their password can be just given to anybody. It's cultural*" as one of the interviewee's argued.

This could also be attributed to other sociodemographic factors such as restricted access to computers in mostly public environments (e.g. schools, Internet cafe's) where users are given a time quota to use computers and thus share passwords to check for any new updates on their accounts on behalf of the user without access [69]. Furthermore, many users especially in rural settings share access to mobile phones, or rely on others e.g. family members for interpretation and help [64]. Specifically women and those with less education, who are less likely to have their own mobile phones [57].

Beyond the demographic divides, there are cultural differences across the continent that determine the prevailing privacy practices [77]. For example, countries in North Africa are usually more conservative and religious. In these countries, religious practices tend to undermine constitutional rights to privacy [40]. Conversely, most countries in Sub-Saharan Africa try to adhere to the constitutional privacy rights stipulated [25,50]; however, it is difficult to make an accurate prediction to what extent they respect users' online privacy since the necessary technology-law enforcement infrastructure, and social organization is often minimal or non-existent[16].

Overall, privacy perceptions and practices are not uniform across African cultures and nations as each is dependent on a variety of factors such as cultural, religious, communal, social, and philosophical factors. As a result, there are no universal privacy practices in Africa. However, many African countries have a hybrid or mixed legal systems formed by interweaving a myriad of distinct international legal instruments and decisions that still find application in many African legal systems [71]. These influence how African online users of online services safeguard and enhance their respective states of privacy. We, therefore, turn to the legal landscape next.

2.3 Privacy Laws in Africa

Most privacy policies and regulations in Africa were established in the 1960s and 1970s during the struggle for independence [41]. However, these regulations did not reflect the value of privacy in an African context, nor did they influence Africans' online privacy consciousness due to little or no technological advances that could lead to the right policy and regulatory responses at the time [41]. As a result, the majority of African countries guarantee constitutional privacy rights in terms of the person, home, and other property, but no guarantees exist regarding information privacy in general or eHealth information privacy in particular. For example, section 14 of the South African constitution stipulates that "*Everyone has the right to privacy, which includes the right not to have – (a) their person or home searched; (b) their property searched; (c)their possessions seized; (d) or their privacy of their communications infringed*" [16]. This is relative to Article 27 of Uganda's constitution [60], and Article 31 of Kenya's constitution [56] among others.

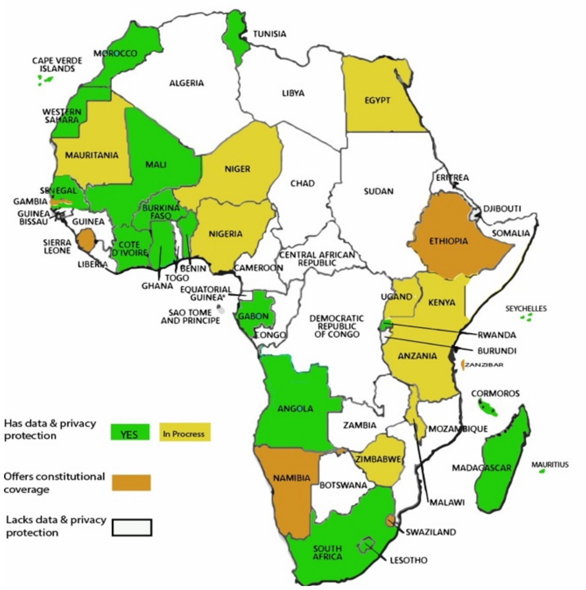

Figure 1: The Africa personal data and privacy protection landscape (Adapted from [22])

Few works have investigated the status of privacy and data protection, or specifically eHealth privacy regulation in Africa [20,40,42,59,71]. Those works have found that eHealth regulation is either non-existent, complex, or fragmented (see Figure 1). Where they exist, national policies are heavily influenced by international legal instruments that regulate privacy and human rights issues [71]. In most cases, even the existing privacy and data protection regulation is ambiguous, underdeveloped, still being drafted, or yet to be passed by the respective legislative bodies [16] (see Figure 1).

Makulilo [41,42] took stock of a number of current African privacy laws and initiatives geared towards the harmonization of data protection policies. The research found that most initiatives are similar yet differ in formulation and details. Policies are mostly vague or open-phrased rules, coupled with a lack of national enforcement bodies. Moreover, some countries like Tanzania belong to multiple regional bodies i.e Tanzania is both a Southern African Development Community (SADC) and an East African Community (EAC) member state. These regional bodies might have different privacy practices and policies, creating challenges in formulation and enforcement of privacy protections given the different legal systems between the groups of countries.

The African Charter on the rights and welfare of the Child 1990 (ARWC) is the only African Union (AU) instrument that expressly guarantees the right to privacy although limited to children: "*no child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honor or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.*" [2,41]. In the recent past, the AU established the *Convention on Cybersecurity and Personal Data Protection 2014* that enacted security rules for electronic transactions, personal data protection, and cybercrimes, to better protect the privacy of citizens across the continent and address the dangers and risks derived from the use of electronic data and individual records in their daily and professional lives [3,4]. However, only ten countries (Benin; Chad; Comoros; Congo; Ghana; Guinea-Bissau; Mauritania; Sierra Leone; Sao Tome & Principe; Zambia) have since signed and two (Mauritius and Senegal) have ratified the cybersecurity convention [4]. The convention needs 15 ratifications to come into force [28].

At a sub-regional level, the Supplementary Act on personal data protection within the Economic Community of West African States (ECOWAS) is the only concrete African sub-regional framework on data and privacy protection [23,41]. It is massively influenced by the now antiquated European Union data protection directive (directive 95/46/EC) [70] and urges each member state to set up a data protection authority to oversee the implementation of the stipulated data protection regulation(s), protect user privacy and promote the free movement of information among member states and non-ECOWAS member states with equally adequate protections [23,41]. It expressly stipulates the rights of persons whose personal data can be subjected to automated or non-automated processing such as the right to information, access, object, rectify and destroy collected data. Data controllers are supposed to confidentially and securely preserve user data for specified durations [23,41].

Similarly, within SADC only 5 Member states [Seychelles; Mauritius; Angola; Lesotho; South Africa] have adopted comprehensive data privacy legislation coupled with a more precise and coherent *Data Protection Model-Law 2012* which includes a particular policy on the automatic and non-automatic processing of both private and public data [11,41].

Correspondingly, in the East African Community (EAC) sub-region, the EAC Legal Framework for Cyber Laws 2008/2011 phase I is a legal framework tailored explicitly towards the harmonization of data and privacy protection policies and regulation within the region [41,45]. Unlike other regional regulations on privacy and data protection, this legal framework is not a model law but instead presents best practice recommendations on data and privacy protection for partner states to consider while formulating and developing their own data, privacy, and cyber regulations. The framework is primarily focused on privacy concerns that pertain to electronic transactions and signatures, data protection and personal privacy, consumer protection and computer crime [45].

As of 2017, Burundi and Kenya had drafted regulation bills with specific provisions on online privacy such as informing users about the purpose(s) for the collection of their personal information e.g. names, ethnic origin, religious affiliation and addresses, the means available to the user to access, modify and or delete such information, and adherence to proper storage measures and security practices [45]. A specific online search for "e-health privacy regulation in Kenya" returns around to twelve documents[1] ranging from the National Constitution, Health Sector Information Systems Policy Act, the National Health Policy Act to the drafted *Data Protection Bill 2012* [29]. However, as noted earlier details within such policies are mostly vague. For example, a policy statement from the National Health Policy Act states that stakeholders are responsible for "*facilitating access to information to the public while protecting privacy and confidentiality*"[44]. In this policy statement, there is no precise definition of what constitutes as relevant information or what the standard is for the protection of privacy.

On the contrary, the Economic Community of Central African states (ECCAS) has the least developed data privacy practices and regulations [29,41] of all the African sub-regional bodies.

Townsend [71] conducted an impact assessment of eHealth Regulation in Africa and found that eHealth has primarily been developed without the benefit of any specific formal law directly tailored to its practice across the continent. This overview of eHealth legal frameworks across 10 African countries (Ivory Coast; Ghana; Kenya; Malawi; Mozambique; Nigeria; Rwanda; Tanzania; Uganda and Zambia) shows that whereas the legal frameworks differ from country to country and between the various African regions, some form of recognition of the right to health is ingrained within the constitutions of all these countries [71]. For example, Article 9 of Ivory Coast constitution stipulates that "*everyone is also entitled to access to healthcare services*" [13] and Nigeria's section 17(3)d stipulates that "*the state shall direct its policy towards ensuring that there are adequate medical and health facilities for all persons*" [49]. Although, these countries have healthcare legislation and medical ethical codes of practice which stipulate that most doctor-patient relationships have to be kept private and confidential, they still have the obligation to progressively adopt and implement new health policies to further safeguard healthcare service quality and accessibility, which may conflict with privacy [71]. The absence of specific eHealth data and privacy protection regulation and or lack of eHealth regulatory bodies shows the intricacies that exist in efforts towards the protection of eHealth privacy across the continent.

Overall, concrete data and privacy protection laws do not exist in most African countries. Only 21 African countries have drafted privacy laws that are greatly influenced by outdated European privacy standards [29]. Consequently, there are no provisions within these laws that expressly address eHealth privacy, hence protections have to be inferred from generic privacy and or healthcare legislation, where available. Thus, there is a need for specific guidelines and policies on the privacy and data protection of eHealth innovations. African countries should review gaps in their legal regimes and institute appropriate measures to address them. Standardization and harmonization of definitions for different data types or concepts such as "sensitive data", "health or personal data" and processes such as establishment of a data agency that would oversee the implementation of data and privacy laws and restrict the inward or outward transfer of personal information beyond the stipulated jurisdictions is required. This would ensure African-centric eHealth privacy protections that would spur the growth and utilization of eHealth initiatives which address the continent's needs for affordable and accessible healthcare. To give practical examples of this, we next turn to current health innovations on the continent and their related privacy issues.

2.4 Case Studies of Social-Media based Health Innovations and their related Privacy Issues

Fayoyin [24] demonstrated the following African use cases of social media interventions used to address multiple health issues through mobile devices held by different population groups across the continent. Additionally, for each case we explain the related privacy implications.

Four daily interactive short messages (SMS) intended to reach an audience 10,000 were sent by organizations such as Oxfam and the United Nations Children's Fund (UNICEF) during a polio outbreak in Somalia. The SMS communicated and provided information about polio immunization. From a privacy perspective, it is interesting to note that no users consented to a subscription to such messages. This example shows us that a focus on digital innovation by development agencies sometimes leads to "pet project syndrome" where they participate in eHealth initiatives solely for agency branding and visibility without seeking user consent in their campaigns. This may lead to half-hatched social media health campaigns or applications. A lack of oversight and co-ordination of such programs can, in turn, lead to the misuse of users' data especially when the project shuts down or ends unexpectedly.

FHI360, a human development nonprofit organization, initiated a social media HIV campaign on platforms such as Facebook, Baidoo, and Grindr in Ghana to promote conversation about specific health issues and to increase utilization of necessary services. They used open and closed Facebook groups to communicate and engage with the members. As a result, 15,4400 unique members largely became predisposed to seek customized services. These groups help members gain a psychological sense of community as they virtually meet with others and overcome social isolation [48]. From a privacy perspective, anonymity within the group is important to address trust and privacy issues that may arise due to the stigma associated with diseases such as HIV. As such, true-name policies on some social media platforms can hamper efforts towards trust building and group cohesion [63]. This can prevent group members from sharing information and engaging with others out of fear that their identities and information will not be protected.

Nigeria effectively coordinated response to the Ebola outbreak using social media campaigns on Twitter and Facebook. These campaigns helped to disseminate accurate information on the signs and symptoms of the disease, counter

[1] https://goo.gl/KekYat

hoax messages, and provide appropriate information nationally and internationally about the outbreak. As a result, only 20 people died, as compared to nearly 8000 and 7000 in Sierra Leone and Liberia, respectively. From a privacy perspective, we note that social media campaigns centered around specific health issues to foster behavioral change often involve an avalanche of messages. These can be intrusive to people, and authorities should therefore carefully consider the tradeoff between the utility of the message and the requisite infringement of users' privacy [65].

Development and health partners established the Mobile Alliance for Maternal Action (MAMA) in South Africa to combat maternal health and childbirth problems. MAMA was used to disseminate culturally sensitive information to expectant mothers through SMS, interactive websites, voicemails on mobile phones and social networks. MAMA includes the platform "Mom Connect[2]," which includes an interactive question and answer portal designed to link pregnant women and mothers to healthcare workers. Over a million mothers and women have been reached through this service. From a privacy perspective, such social media-based health platforms provide the ability to track patients through treatment initiation processes used to monitor medication adherence. These tracking activities involve detecting patients who are at risk of loss to follow-up and reminding them about their health care treatments. In addition, these platforms enable medical personnel to perform operational research at reduced costs, as valuable medical data is extracted from these applications and utilized for research purposes. Again, the benefit of these medication adherence schemes and the use of data for research has to be weighed against the potential privacy implications of extensive patient tracking [65].

In a bid to make healthcare facilities more accessible and searchable using smartphones, location-based eHealth applications such as myDawa[3], HelloDoctor[4] and Vula[5] have been developed and are utilized by both patients and doctors for consultations, referrals, search for the closest health centers, making of appointments, and obtaining and updating patient medical records. In the same vein, there are also smart medical devices such as Matibabu[6] used for bloodless malaria testing, and the Eva system used to take cervical selfie's to visually screen and inspect cervical cancer in health facilities or mobile outreaches with use in over 26 countries such as The Gambia and Ethiopia [46]. Accordingly, doctors are able to remotely consult with peers, superiors, or outside experts through the remote consultation features provided by some of these applications. Hence, these applications have great user privacy implications especially if user information such as test results and cervical images contain personal identifiable information and are shared with other third-party organizations that may want to know and learn about it [6].

3 RESEARCH AGENDA

The advancement of eHealth services has shown the potential to benefit the lives of many Africans. Despite that and given the rate at which these innovations have been developed, privacy and data protection has not been considered at the onset of implementation. Albeit these health innovations benefit from the power of social connections and easy information disclosure, these benefits at the same time present serious risks to users' privacy [65]. Users may be convinced of the benefits of adopting emerging solutions, but ultimately they may jeopardize their privacy with no legal protections in place to help them. What if an app or website goes out of business and all of their data is lost? What if a users' patient identifier is sold to marketers? What sort of information is disclosed in a text message or on social media particularly when a device is shared by the family?

Given the varying privacy perceptions and practices across African cultures and the nascent state of legal protections, we call for a comprehensive effort to address the privacy challenges of eHealth innovations in Africa.

There are several privacy-related challenges centered around information collection, processing, and sharing that should be addressed. Doctors use proprietary platforms (e.g. Facebook, WhatsApp) for conversations about patients, but these platforms store the data for an indefinite amount of time, and/or claim ownership over the data. There are laws about the transmission and use of patient data, but doctors and healthcare professionals may ignore them given the lack of oversight with little to no enforcement [31] despite the resolute global push for such regulations to enable governments to catch up with the ways their citizens are engaging with technology.

Even if users opt to use specialized eHealth services, most eHealth applications are not encrypted, and their communications can easily be intercepted. Although there are humanitarian projects aimed at improving healthcare, there are instances where data is collected about patients for research without their knowledge and stored outside their jurisdictions where different privacy rules might apply.

Moving towards viable solutions would require addressing issues such as inadequate legal protections, limited precautions by healthcare providers and poor technical design to mitigate risks and better protect users. Therefore, we propose a pan-African research agenda to study (and eventually shape) the continent's perspectives on eHealth privacy. Our proposed methodology for this research agenda includes two main elements: the collection and analysis of publicly available literature, and an online behavioral study to gather direct input from people across all African countries.

In the initial phase, we will work towards understanding the existing 'state of privacy' by creating a database of privacy policies throughout the region to observe any trends and, distinctions among countries., and differences in how eHealth data is regarded. The information collected here will help to guide the design of the online survey to ensure we obtain information that is relevant. Simultaneously, we will establish connections with key stakeholders and researchers who have

[2] http://www.health.gov.za/index.php/mom-connect
[3] https://www.mydawa.com/#/home
[4]https://www.hellodoctor.co.za/
[5] http://www.vulamobile.com/
[6] http://matibabu.thinkitlimited.com/

worked on privacy-related projects in the region, to ensure that robust and actionable recommendations and guidance are generated, and to maximize their uptake. The next phase involves conducting an online contextual study to collect information regarding attitudes towards privacy and privacy-related behaviors (cf. [35]). The goal here is to evaluate differences in privacy attitudes and behaviors.

We envision the outcomes of this research agenda to have both legal implications and design implications. On the legal side, our results can inform and advise the African continent to develop a pan-African legal framework, much like the GDPR in Europe, that will increase the cohesion of eHealth privacy regulations on the African continent. On the design side, our results can provide guidelines for eHealth innovators seeking to market their products and services in African nations to address the extant regulations and the privacy concerns of users in their applications. We address each of these implications in more detail below.

4 LEGAL IMPLICATIONS

This section addresses existing regulatory frameworks that can be adopted or adapted in Africa. The results of our research agenda will determine to what extent the African framework will borrow from these existing approaches.

4.1 United States (US) Legal Framework for Health Privacy

In the United States, the 1996 Health Insurance Portability and Accountability Act (HIPAA) is the primary law concerning health information privacy [74]. HIPAA provides protection for patients in the event of privacy violations from health care providers. This framework is designed to protect personally identifiable health Information, which includes medical records (both paper and electronic), personal communications, and electronic communications (email and faxes). HIPAA requires certain entities to obtain patient authorization before sharing PHI. Covered entities under HIPAA include healthcare providers (doctors, nurses, pharmacists), healthcare facilities (hospitals, clinics, stand-alone healthcare facilities), health plans (HMOs, insurers, Medicare/Medicaid), and health information clearing houses (billing services, community health information systems) [73].

A framework similar to HIPAA would be beneficial for the African continent in many ways. Its tiered levels of privacy allow varying levels of information to be released depending on local and state laws. This approach goes beyond a cookie cutter approach to privacy and acknowledges the need for adjustments based on cultural norms and practices of respective African countries. However, greater measures will need to be employed to increase understanding of privacy laws to (a) reduce the burden on companies and increase their willingness to adopt and (b) make it less confusing for the everyday user and create better awareness of how to identify and report violations.

Furthermore, while HIPAA standards allow protections for users’ privacy, “covered entities” are limited and instances where data is collected and shared by individuals, such as in mobile health apps, may not be covered [6,8,67]. In light of our analysis of eHealth in Africa, it is thus imperative that a legal framework for African countries goes beyond HIPAA and acknowledges various data flow channels to have a wider scope and account for different technologies that collect health data.

Table 1 : Comparison of the US Vs EU privacy frameworks.

	HIPAA	GDPR
Protected Information	Any data from which a living individual is identified or identifiable, whether directly or indirectly	Any individually identifiable information relating to past, present or future physical or mental health condition, the provision of health care or the payment of health care
Jurisdiction	Covers entities and business associates within the United States, including non-United States citizens or residents.	Applies to organizations that process personal data of individuals based in the EU and either (i) monitors the behavior of data subjects within the EU, or (ii) offers goods or services to individuals within the EU.
Covered Entities	Health care providers who electronically transmit personal data about certain HIPAA-covered transactions (e.g., electronically bills of a health plan), a health plan, or a health care clearinghouse	Goes beyond healthcare providers and includes any organization that processes online data. See “Jurisdiction” for the scope covered.
Enforcement	Carried out by several governmental organizations (e.g. FCC, HIPAA)	Carried out by one authority across all member states
Consent	Covered entities may choose to request consent disclosures of health data for 1) treatment, 2) payment, and 3) healthcare operations	Health data can only be accessed 1) with explicit consent from the individual, 2) for health and social care, and 3) for public health
Data Storage	Data could be kept as long as companies deem necessary according to their respective policies	EU citizens have the ‘right to be forgotten’

4.2 European Legal Framework for Health Privacy

The European (EU) General Data Protection Regulation (GDPR) is a collection of legislation concerning online data privacy that went into effect across the entirety of the EU on May 25, 2018. Unlike HIPAA, the GDPR covers a broad wide scope of "Personally Identifiable Information" such as race, biometrics data, and sexual orientation which may fall outside the scope of HIPAA [7]. The GDPR not only applies to organizations located within the EU but it also includes organizations outside of the EU that offer goods or services to or monitor the behavior of EU users. It is important to note that regardless of the company's location, once companies process and/or hold the personal data of EU citizens GDPR would apply. This provides a strong incentive for African nations seeking to provide services in the EU to follow GDPR in their own laws. For a summary of the major differences between HIPAA and the GDPR (Table 1).

The implementation of the GDPR implied that all European Union (EU) member states had to eventually repeal local or existing privacy laws. In the African context, this may be advantageous regarding outdated protections, but cumbersome for certain countries with opposing views and cultural values on the perception of privacy and health data. Therefore, should our research agenda indeed find strong differences in privacy protection across Africa, then it may be better to adopt regulation that allows more flexibility for local laws to be enforced on a case to case basis as the need arises. This would increase the chance of success of the pan-African privacy framework, as it would allow for flexibility in the negotiations among countries

4.2 Towards an African Legal Framework for Health Privacy

While international legal frameworks provide a good base for establishing an African-centric privacy framework, it is important to not simply copy other frameworks established from other countries and assume that it would work in Africa. Forthcoming legal frameworks for the African continent should reflect the nuanced customs, privacy attitudes, perceptions, and local needs to best serve the people it is intended to protect. Furthermore, legislators could use available frameworks such as HIPAA and GDPR as a foundation but should consider crafting a hybrid approach to create a solution that is appropriate for African nations. For instance:

4.2.1 Regulatory bodies: Similar to HIPAA, having regulatory bodies in each African country may be useful for disseminating tailored decisions and providing guidelines.

4.2.2 Scope and Definition: Narrowing the definition of sensitive information (e.g. what is included in "health data") while broadening the scope of data flow (e.g. what is considered "transmission" and "disclosure") could provide more protections for users but it is important to involve stakeholders from various countries in the negotiation process.

4.2.3 Regulatory Clarity: Healthcare practitioners (e.g. doctors, nurses, counsellors, pathologists) and providers (e.g. hospitals, pharmacies, universities), eHealth developers, and users need to be provided with adequate support for the continued development of innovative solutions. Likewise, users and should be educated about the regulatory status of the applications they use, their rights and the process needed to file complaints.

Additionally, we must consider the advancement of technology and how that impacts data types, data processing, and data flow across general healthcare practitioners and national borders as information held within an eHealth infrastructure is generally distributed. Cloud computing allows data to be collected from one location but processed in another, which could have implications for jurisdictions with less than adequate protections. Dedicated data centers for cloud computing services should avoid creating "data havens" and instead provide equivalent levels of data protections, so that information can be passed between African countries (and beyond) without restrictions. Therefore, establishing standardized data protection laws across countries could assist in enabling a free and safe flow of data across national borders.

5 DESIGN IMPLICATIONS

The advent of eHealth and the need for the protection of its users calls for the exploration of users' perceptions of and behavior towards privacy to ensure that systems in the future can be designed with these factors in mind.

5.1 Perceptions and Practices

As noted in prior work, unless eHealth systems are carefully designed to preserve an individual's privacy, their prevalence may decrease the level of individual privacy afforded during and beyond a healthcare encounter [17]. For a region that is steadily enjoying the benefits of new eHealth solutions, maintaining user privacy may reduce vulnerabilities that could stifle innovation. However, a fundamental step towards establishing an actionable privacy framework that would shape system design is investigating how users define privacy. Privacy attitudes and perceptions can be influenced by many factors including culture [35], social norms [9,51], and contextual factors [32,33,50]. Equally important, individuals often make decisions based on the expectation of loss of privacy and the potential gain of disclosure; user's final privacy behavior is usually based on the expected outcome of the tradeoff [22]. Researchers and developers should consider these factors to assist the privacy decision-making process by matching users' expectations and mental models of privacy designs [18,36].

5.2 Risks, Implications, and Recommendations

Health data is valuable. Information collected by an eHealth device (e.g., wearable) or associated application is believed to be worth ten times that of a credit card or social security number on a black market and among the most breached into [37]. Disclosing personal health information makes users vulnerable to a myriad of privacy risks. At the same time, people may find themselves in situations where they disclose health related information through social networking applications—even though some may express wanting more privacy. This concept is based on the privacy paradox [15] which implies that while people express concerns about privacy, they continue to behave in ways that contradict what they express. How can we use this concept to address some of the eHealth privacy challenges that users are currently facing? How can we protect users' privacy without compromising the e-health system's functionality? As a step towards African-centric privacy framework, we offer the following recommendations:

5.2.1 Do no harm: Designers and developers should consider collecting as little information as possible about users that is needed for the application to function as possible. For example, Orange Cameroon's MyHealthline is an SMS based service that provides personalized medical advice on contraception, Malaria, HIV/AIDS and STDs by allowing users to text questions which will be answered by local doctors and nurses [53]. Confidentiality and anonymity are maintained by not disclosing identifying information about users but rather focusing on the responses to health-related questions. Hence, they provide useful health information and at the same time preserve user's privacy while users remain anonymous [53].

5.2.2 Transparency matters: Disclosing data collection and data sharing practices could potentially improve users' trust in the system. For example, illustrating privacy policies in an easy to understand format (e.g. removing legal jargon and not using long standard privacy policies) could increase user comprehension of their privacy rights and practices; hence increasing transparency. Designers should consider creating a standardized privacy policy presented in an easy to understand format: bulleted, graphical, or tabular layout to avoid information overload from lengthy bodies of text [54,55,67].

5.2.3 Improve Awareness: Develop mechanisms so that users are aware of what data is considered sensitive and how to maintain control over this information. Volk et. al recommends carefully listing the types of data being shared and presenting the information in a manner that users could easily make changes to data sharing preferences and identify the status of data sharing for specific data types (such as a toggle button that allows one to stop sharing glucose levels) [76].

5.2.4 Increasing Control: Users should have the option to sign up for options than may be privacy invasive rather than being opted-in by default since many users may not bother changing the default option. The persuasive effect of default options can influence user behavior and it is important that users are aware of what they are agreeing to [65]. Users should also be given the opportunity to decide what information an e-health application or service can collect of them and whom this information can be shared with. This would also necessitate allowing users to access and use the basic forms of the service if they do not feel comfortable disclosing information instead of completely denying them service. Therefore, user control should be considered when designing User Interfaces (UI) that concern privacy settings.

6 LIMITATIONS AND FUTURE WORK

An obvious limitation to our work is the complete reliance on previously published privacy, eHealth and legal research literature, blogs, websites and mobile applications that we were able to access through general web searches and or special publication databases e.g. ACM Digital Library, Guide to Computing Literature, IEEE Xplore and Springer among others. Therefore, we are likely to have missed out on literature that did not come to our purview or simply is not online. This was further impacted by the small number of research studies that have been done so far on this topic within an African- centric context.

It is also important to note that the African personal data and privacy regulatory landscape is evolving as a number of African countries continue to enact new data and privacy protections. Therefore, the privacy landscape might no longer be as reflected in this work by the time of publication. However, in future work, researchers can leverage the insights provided by our work to advance their own eHealth and privacy research agendas in Africa.

Future research should also explore challenges regarding more contextual privacy decisions, as well as data portability, and how designs could be integrated into eHealth solutions. For instance, if an entity (e.g., health care provider, eHealth manufacturer) legitimately shares data with a firm (neutral, third party) that encounters a change in ownership, how can end users be notified and made aware of what will happen to their data? Additionally, improving the visibility of potential privacy risks may be helpful in reducing exposure. Researchers or developers could consider establishing systems to monitor and identify what types of data are generated by eHealth applications and presents risks to users.

7 CONCLUSION

In this work, we proposed a research agenda to investigate the effect of cultural, constitutional, and societal factors on eHealth privacy concerns and preferences among the different African countries. We find that there are no universal privacy practices and social media in Africa is integral to citizens getting adequate healthcare, but privacy issues may thwart these benefits. It is therefore important to have an African legal framework for eHealth privacy that will ensure data and privacy protections across the continent. This will facilitate innovation that would continue to decrease the cost and access to healthcare.

ACKNOWLEDGEMENTS

We would like to thank the authors whose published literature we reviewed to garner an understanding of the prevailing privacy perceptions and practices across the African continent. MN was supported by a Facebook Emerging Scholar Award.

REFERENCES

1. Rediet Abebe, Shawndra Hill, Jennifer Wortman Vaughan, Peter M. Small, and H. Andrew Schwartz. 2018. Using Search Queries to Understand Health Information Needs in Africa. In *Neural Information Processing Systems 30 (NIPS 2018).* Retrieved June 20, 2018 from http://arxiv.org/abs/1806.05740
2. African Union. 1990. *The African Charter on the Rights and Welfare of the Child.* African Commission on Human and People's Rights, Addis Ababa, Ethiopia. Retrieved June 22, 2018 from

http://www.achpr.org/files/instruments/child/achpr_instr_charterchild_eng.pdf

3. African Union. 2014. *African Union Convention on Cyber Security and Personal Data Protection.* The twenty-third Ordinary Session of the Assembly, Malabo, Equatorial Guinea. Retrieved June 22, 2018 from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
4. African Union. 2014. *African Union Convention on Cyber Security and Personal Data Protection.* The twenty-third Ordinary Session of the Assembly, Malabo, Equatorial Guinea. Retrieved June 22, 2018 from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
5. Jocelyn Olivia Todd Anstey Watkins, Jane Goudge, Francesc Xavier Gómez-Olivé, and Frances Griffiths. 2018. Mobile phone use among patients and health workers to enhance primary healthcare: A qualitative study in rural South Africa. *Social Science & Medicine* 198: 139–147. https://doi.org/10.1016/j.socscimed.2018.01.011
6. Shifali Arora, Jennifer Yttri, and Wendy Nilsen. 2014. Privacy and Security in Mobile Health (mHealth) Research. *Alcohol Research : Current Reviews* 36, 1: 143–151.
7. Sean Baird. 2017. GDPR matchup: The Health Insurance Portability and Accountability Act. *IAPP: Privacy Tracker.* Retrieved July 2, 2018 from https://iapp.org/news/a/gdpr-match-up-the-health-insurance-portability-and-accountability-act/
8. Syagnik Banerjee, Thomas Hemphill, and Phil Longstreet. 2018. Wearable devices and healthcare: Data sharing and privacy. *The Information Society* 34, 1: 49–57. https://doi.org/10.1080/01972243.2017.1391912
9. Louise Barkhuus. 2012. The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12), 367–376. https://doi.org/10.1145/2207676.2207727
10. Stephanie Baum. 2017. Startup seeking to offer WhatsApp for healthcare plans expansion to South Africa next year. *MedCity News.* Retrieved July 2, 2018 from https://medcitynews.com/2017/11/startup-seeking-offer-whatsapp-healthcare-plans-expansion-south-africa-next-year/
11. Jean-Francois Le Bihan, Ida Jallow, Sandro Bazzanella, Hiwot Mulugeta, and Brahima Sanou. 2013. *Data Protection: Southern African Developement Community (SADC) Model Law.* International Telecommunication Union (ITU). Retrieved June 22, 2018 from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf
12. Joaquin A. Blaya, Hamish S.F. Fraser, and Brian Holt. 2010. E-Health Technologies Show Promise In Developing Countries. *Health Affairs* 29, 2: 244–251. https://doi.org/10.1377/hlthaff.2009.0894
13. Nicolas Boring. 2016. Côte d'Ivoire: New Constitution Adopted. *Global Legal Monitor.* Retrieved from https://www.loc.gov/law/foreign-news/article/cte-divoire-new-constitution-adopted/
14. Patricia Boshe. 2016. Data Privacy Law Reforms in Tanzania. In *African Data Privacy Laws.* Springer, Cham, 161–187. https://doi.org/10.1007/978-3-319-47317-8_8
15. Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science* 4, 3: 340–347. https://doi.org/10.1177/1948550612455931
16. Lee A. Bygrave. 2010. Privacy and data protection in an international perspective. *Scandinavian studies in law*, 56: 165–200.
17. Kelly Caine and Rima Hanania. 2013. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association* 20, 1: 7–15. https://doi.org/10.1136/amiajnl-2012-001023
18. Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring Internet Security Perceptions and Practices in Urban Ghana. In *Symposium on Usable Privacy and Security (SOUPS 2014)*, 136. Retrieved from https://www.usenix.org/sites/default/files/soups14_proceedings.pdf#page=136
19. Constitutional Assembly. 1996. *The Constitution of the Republic of South Africa, Act 108 of 1996.* Minister for Justice and Constitutional Development. Retrieved from http://www.wipo.int/edocs/lexdocs/laws/en/za/za107en.pdf
20. Deloitte. 2017. *Privacy is Paramount: Personal Data Protection in Africa.* Johannesburg, South Africa. Retrieved July 1, 2018 from https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf
21. Digital Health. 2018. WhatsApp doc: Legal and practical perspectives of using mobile messaging. *Digital Health.* Retrieved July 2, 2018 from https://www.digitalhealth.net/2018/02/whatsapp-doc-legal-and-practical-perspectives-of-using-mobile-messaging/
22. Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. 2006. Privacy calculus model in e-commerce – a study of Italy and the United States. *European Journal of Information Systems* 15, 4: 389–402. https://doi.org/10.1057/palgrave.ejis.3000590
23. Economic Community of West African States. 2011. *Directive fighting cyber crime within ECOWAS.* Abuja, Nigeria. Retrieved June 22, 2018 from https://www.ccdcoe.org/sites/default/files/documents/ECOWAS-110819-FightingCybercrime.pdf
24. Adebayo Fayoyin. 2016. Engaging Social Media for Health Communication in Africa:Approaches, Results and Lessons. *Journal of Mass Communication & Journalism* 6, 6: 1–7. https://doi.org/10.4172/2165-7912.1000315
25. Tom Ferguson. 2002. From patients to end users: Quality of online patient networks needs more attention than quality of online health information. *BMJ* 324, 7337: 555–556. https://doi.org/10.1136/bmj.324.7337.555
26. Anastasia J. Gage. 2007. Barriers to the utilization of maternal health care in rural Mali. *Social Science & Medicine* 65, 8: 1666–1682. https://doi.org/10.1016/j.socscimed.2007.06.001
27. Kurubaran Ganasegeran, Pukunan Renganathan, Abdul Rashid, and Sami Abdo Radman Al-Dubai. 2017. The m-Health revolution: Exploring perceived benefits of WhatsApp use in clinical practice. *International Journal of Medical Informatics* 97: 145–151. https://doi.org/10.1016/j.ijmedinf.2016.10.013
28. Graham Greenleaf. 2017. *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey.* UNSW Law Research Paper No. 17-45, Rochester, NY. Retrieved June 19, 2018 from https://papers.ssrn.com/abstract=2993035
29. Graham Greenleaf. 2017. *Global Tables of Data Privacy Laws and Bills (5th Ed 2017).* Social Science Research Network, Rochester, NY. Retrieved June 19, 2018 from https://papers.ssrn.com/abstract=2992986
30. Kate Hampshire, Gina Porter, Samuel Asiedu Owusu, Simon Mariwah, Albert Abane, Elsbeth Robson, Alister Munthali, Ariane DeLannoy, Andisiwe Bango, Nwabisa Gunguluza, and James Milner. 2015. Informal m-health: How are young people using mobile phones to bridge healthcare gaps in Sub-Saharan Africa? *Social Science & Medicine* 142: 90–99. https://doi.org/10.1016/j.socscimed.2015.07.033
31. Janine Hiller, Matthew S. McMullen, Wade M. Chumney, and David L. Baumer. 2011. Privacy and Security in the Implementation of Health Information Technology (Electronic Health Records): U.S. and EU Compared. *Boston University Journal of Science & Technology Law* 17: 1–39.
32. Gordon Hull, Heather Richter Lipford, and Celine Latulipe. 2011. Contextual gaps: privacy issues on Facebook. *Ethics and Information Technology* 13, 4: 289–302. https://doi.org/10.1007/s10676-010-9224-8
33. Ashraf Khalil and Kay Connelly. 2006. Context-aware telephony: privacy preferences and sharing patterns. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, 469–478. https://doi.org/10.1145/1180875.1180947
34. Brenda Kubheka. 2017. Ethical and legal perspectives on use of social media by health professionals in South Africa. *South African Medical Journal* 107, 5: 386–389. https://doi.org/10.7196/samj.2017.v107i5.12047
35. Yao Li, Alfred Kobsa, Bart P Knijnenburg, and MH Carolyn Nguyen. 2017. Cross-Cultural Privacy Prediction. *Proceedings on Privacy Enhancing Technologies* 2: 93–112.
36. B. Lowens, V. G. Motti, and K. Caine. 2017. Wearable Privacy: Skeletons in The Data Closet. In *2017 IEEE International Conference on Healthcare Informatics (ICHI)*, 295–304. https://doi.org/10.1109/ICHI.2017.29
37. Teena Maddox. 2015. The dark side of wearables: How they're secretly jeopardizing your security and privacy. *TechRepublic.* Retrieved June 28, 2018 from https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/
38. Mafika. 2017. The Constitution of South Africa. *Brand South Africa.* Retrieved June 22, 2018 from https://www.brandsouthafrica.com/governance/constitution-sa-glance/the-constitution-of-south-africa
39. Daniel Makina. 2017. Introduction to the financial services in Africa special issue. *African Journal of Economic and Management Studies* 8, 1: 2–7. https://doi.org/10.1108/AJEMS-03-2017-149
40. Alex B. Makulilo. 2012. Privacy and data protection in Africa: a state of the art. *International Data Privacy Law* 2, 3: 163–178. https://doi.org/10.1093/idpl/ips014
41. Alex B. Makulilo. 2015. Myth and reality of harmonisation of data privacy policies in Africa. *Computer Law & Security Review* 31, 1: 78–89. https://doi.org/10.1016/j.clsr.2014.11.005
42. Alex B. Makulilo. 2016. The Context of Data Privacy in Africa. In *African Data Privacy Laws.* Springer, Cham, 3–23. https://doi.org/10.1007/978-3-319-47317-8_1
43. Ignacio Mas and Olga Morawczynski. 2009. *Designing Mobile Money Services Lessons from M-PESA.* Retrieved June 28, 2018 from https://www.mitpressjournals.org/doi/pdf/10.1162/itgg.2009.4.2.77
44. Ministry of Health. 2014. *Kenya Health Policy 2014-2030: Towards attaining the highest standard of health.* Ministry of Health, Nairobi, Kenya. Retrieved June 22, 2018 from

http://publications.universalhealth2030.org/uploads/kenya_health_policy_2014_to_2030.pdf

45. Anne Miroux, Cecile Barayre, and Torbjorn Fredriksson. 2013. *Harmonizing Cyberlaws and Regulations: The experience of the East African Community.* United Nations Conference on Trade and Development, New York and Geneva. Retrieved June 22, 2018 from http://unctad.org/en/PublicationsLibrary/dtlstict2012d4_en.pdf
46. MobileODT. 2012. EVA System: A turnkey solution for visual-based medical procedures. *MobileODT.* Retrieved July 2, 2018 from https://www.mobileodt.com/eva-system/
47. Kathryn C Montgomery, Jeff Chester, and Katharina Kopp. 2016. *Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection.* Center for Digital Democracy, American University. Retrieved from https://www.democraticmedia.org/sites/default/files/field/public/2016/aucdd_wearablesreport_final121516.pdf
48. Avuya Mxoli and Nicky Mostert-Phipps. 2016. Risks and Benefits of Social Computing as a Healthcare Tool. *Proceeding of International Multi-Conference on Complexity, Informatics and Cybernetics.* Retrieved from http://www.iiis.org/CDs2016/CD2016Spring/papers/HB329XQ.pdf
49. Nigerian Parliament. 1999. *Constitution of the Federal Republic of Nigeria.* International Center for Nigerian Law. Retrieved June 22, 2018 from http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm
50. Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79: 119–157.
51. Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press, Stanford, CA. Retrieved September 24, 2013 from http://books.google.com.sg/books?hl=en&lr=&id=_NN1uGn1Jd8C&oi=fnd&pg=PR7&dq=Privacy+in+Context:+Technology,+Policy,+an+d+the+Integrity+of+Social+Life&ots=_J9lXtm4CQ&sig=uwEmoieGtVJQhegXvrT7TryaTrg
52. Melvin Obadha, Andrew Seal, and Tim Colbourn. 2018. Mobile money increasing healthcare access. *Mobile money increasing healthcare access.* Retrieved June 7, 2018 from https://www.scidev.net/sub-saharan-africa/health/opinion/mobile-money-increasing-healthcare-access.html
53. Orange Healthcare. 2014. "My Healthline": Orange's first healthcare hotline in Cameroon. *Orange Healthcare.* Retrieved July 1, 2018 from http://healthcare.orange.com/en/Press-and-medias/Press-releases/2014-Press-Releases/My-Healthline-Orange-s-first-healthcare-hotline-in-Cameroon
54. A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis. 2018. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* 6: 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522
55. Lisa Parker, Tanya Karliychuk, Donna Gillies, Barbara Mintzes, Melissa Raven, and Quinn Grundy. 2017. A health app developer's guide to law and policy: a multi-sector policy analysis. *BMC Medical Informatics and Decision Making* 17, 1. https://doi.org/10.1186/s12911-017-0535-0
56. Parliamentary Select Committee (PSC) and Committee of Experts. 2010. *Constitution of Kenya.* Kenya Parliament. Retrieved June 18, 2018 from http://kenyalaw.org/kl/index.php?id=398
57. Jacob Poushter and Russ Oates. 2015. *CellPhones in Africa: Communication Lifeline.* Pew Research Center, Washington, DC. Retrieved from http://www.pewglobal.org/files/2015/04/Pew-Research-Center-Africa-Cell-Phone-Report-FINAL-April-15-2015.pdf
58. Matthew Price, Erica K. Yuen, Elizabeth M. Goetter, James D. Herbert, Evan M. Forman, Ron Acierno, and Kenneth J. Ruggiero. 2013. mHealth: A Mechanism to Deliver More Accessible, More Effective Mental Health Care. *Clinical Psychology & Psychotherapy* 21, 5: 427–436. https://doi.org/10.1002/cpp.1855
59. Privacy International and National Coalition of Human Rights Defenders. 2018. State of Privacy Kenya. *Privacy International.* Retrieved June 21, 2018 from http://www.privacyinternational.org/state-privacy/1005/state-privacy-kenya
60. Privacy International and Unwanted Witness. 2018. State of Privacy Uganda. *Privacy International.* Retrieved June 21, 2018 from http://privacyinternational.org/state-privacy/1013/state-privacy-uganda
61. S. Rokadiya, J. A. McCaul, D. A. Mitchell, and P. A. Brennan. 2016. Leading article: Use of smartphones to pass on information about patients - what are the current issues? *British Journal of Oral and Maxillofacial Surgery* 54, 6: 596–599. https://doi.org/10.1016/j.bjoms.2016.04.020
62. Jane Sarasohn-Kahn. 2008. The Wisdom of Patients: Health Care Meets Online Social Media. Retrieved May 21, 2018 from https://books.google.com/books/about/The_Wisdom_of_Patients.html?id=tIeqOgAACAAJ
63. Sandra Schmitz. 2013. Facebook's Real Name Policy: Bye-Bye, Max Mustermann? 15.
64. Araba Sey. 2009. Exploring mobile phone-sharing practices in Ghana. *info* 11, 2: 66–78. https://doi.org/10.1108/14636690910941894
65. N. Craig Smith, Daniel G. Goldstein, and Eric J. Johnson. 2013. Choice Without Awareness: Ethical and Policy Implications of Defaults. *Journal of Public Policy & Marketing* 32, 2: 159–172. https://doi.org/10.1509/jppm.10.114
66. StatCounter. 2018. Social Media Stats Africa. *StatCounter Global Stats.* Retrieved July 2, 2018 from http://gs.statcounter.com/social-media-stats/all/africa
67. Ali Sunyaev, Tobias Dehling, Patrick L. Taylor, and Kenneth D. Mandl. 2015. Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association* 22, e1: e28–e33. https://doi.org/10.1136/amiajnl-2013-002605
68. Tamara Taggart, Mary Elisabeth Grewe, Donaldson F Conserve, Catherine Gliwa, and Malika Roman Isler. 2015. Social Media and HIV: A Systematic Review of Uses of Social Media in HIV Communication. *Journal of Medical Internet Research* 17, 11. https://doi.org/10.2196/jmir.4387
69. Matti Tedre and Bukaza Chachage. 2008. University Students' Attitudes Towards e-security Issues: A Survey Study in Tumaini University, Tanzania. http://hdl.handle.net/20.500.11810/2378
70. The European Parliament. 1995. *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* European Parliament, Kirchberg, Luxembourg. Retrieved June 23, 2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046
71. Beverley Townsend. 2015. *mHealth Regulation Impact Assessment: Africa.* GSMA, South AFRICA. Retrieved June 22, 2018 from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/03/003-GSMA-RIA-Africa-27feb15.pdf
72. Beverley Alice Townsend. 2017. Privacy and data protection in eHealth in Africa -an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health care in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking? University of Cape Town, Cape Town, South Africa. Retrieved July 2, 2018 from https://open.uct.ac.za/handle/11427/25510
73. US Department of Health & Human Services. 2015. Covered Entities and Business Associates. *Health Information Privacy.* Retrieved July 2, 2018 from https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html
74. U.S. Government Printing Office. 1996. *Insurance Portability and Accountability Act of 1996.* 104th US Congress, Washington, D.C. Retrieved June 18, 2018 from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/content-detail.html
75. Lavanya Vasudevan, Kelsey Zeller, and Alain Labrique. 2018. Mobile Health. In *Digital Health.* Springer, USA, 15–25. https://doi.org/10.1007/978-3-319-61446-5_2
76. Mojca Volk, Janez Sterle, and Urban Sedlar. 2015. Safety and Privacy Considerations for Mobile Application Design in Digital Healthcare. *International Journal of Distributed Sensor Networks* 11, 10: 549420. https://doi.org/10.1155/2015/549420
77. Tobias Wacker, Lilian Tse, and Chiara Diana. 2017. *mHealth Design ToolKit: Ten principles to launch, develop and scale mobile health services in emerging markets.* GSMA mHealth Program, frog, London, U.K. Retrieved June 11, 2018 from https://www.gsma.com/mobilefordevelopment/mhealth/mhealth-design-toolkit/
78. Mobile for Development - mHealth. Retrieved June 11, 2018 from https://www.gsma.com/mobilefordevelopment/mhealth/
79. State of Privacy South Africa. *Privacy International.* Retrieved June 21, 2018 from http://privacyinternational.org/state-privacy/1010/state-privacy-south-africa