International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 10, Number 1 (2018), pp. 1-9

http://www.irphouse.com

A Bio-Data Privacy Protection Framework for the Telecommunications Industry in Kenya

Dr. Stanley Githinji[1], Adrian Kamotho Njenga[2], Christopher Mwendwa Katuu[3]

[1] Information Security and Forensics Faculty, School of Science and Technology, USIU-A, Nairobi, Kenya.
[2] Lecturer, Department of Computer Science, Kenya Methodist University, Nairobi, Kenya.
[3] Msc Computer Information Systems student, Department of Computer Science, Kenya Methodist University, Nairobi, Kenya.

Abstract

Privacy is a basic human need which should be protected legally. Right to privacy provides individuals capability of determining to what extent their personal information shall be communicated to others. The concept of privacy figures prominently in discourse about the social and political threats posed by modern information and communications technology (ICT). This paper presents the results of a descriptive survey that sought to examine privacy issues concerning bio-data in the telecommunications sector in Kenya and subsequently develop a framework to address the challenges. This study concluded that although organizations in the telecommunications sector had adopted several bio data privacy protection measures, these measures had not completely translated to absolute bio data privacy. A bio data privacy protection framework was consequently developed for validation by telecommunication industry players. The proposed framework provides increased security for bio data processed and otherwise held by telecommunication firms. It is recommended that telecommunication firms must understand the privacy and security regulations that apply to the customers' bio data they receive, store, process, and transmit. Further, having a robust control framework and implementing it throughout the organization and the third parties can help the telecommunication operators ensure adequate bio data privacy.

Keywords: bio data; privacy; protection; threats; telecommunications

I. INTRODUCTION

The Communication industry is gaining popularity and importance in many advanced and developing countries. Today, communication is becoming the nerve of the life. Mobile usage is growing rapidly, and telecommunication firms are developing new strategies to take advantage of the potential customers [1]. With this reality, privacy of customers' bio data inevitably is an issue of concern. There are many conceptions of privacy and the term is invoked to cover a wide range of interests depending on the commentator. Warren and Brandeis wrote an article entitled *The Right to Privacy* which is often credited as the first publication to establish the philosophical grounds for a right to privacy and for over 125 years, privacy has been viewed as a natural right with individuals desiring the protection of their personal lives and information [2].

Privacy and data protection concerns are distinct issues that arise in any electronic platform especially telecommunication systems. Transactions and personal data are transmitted through mobile phone networks, handled more often by third parties such as agents, and accessed remotely by customers and financial institution employees, the risk of inappropriate access and usage rises. Besides the technological aspect, consumers' lack of education and lack of experience with formal financial services and technology may raise data security risks [3].

The telecommunications firms deal with large amounts of data. When used effectively, this big data enables the telecommunication firms to achieve efficiency and profitability across the entire telecommunications value chain. However, the potential advantage of big data may be tempered by increasing privacy concern among users [4]. Data has become a resource of important economic and social value and the exponentially growing amount of data that is generated, shared, transmitted, and accessed, together with new technologies and analytics available, opens up new and unanticipated uses of information. Furthermore, the collection of large and multifaceted data sets and the new possibilities of their use lead to growing privacy concerns. The disclosure and use of bio data is increasingly associated with fear, uncertainty, or doubt [5]. Users are concerned about privacy and that large amounts of their personal information may be tracked and made accessible for other purposes to other users [6].

Telecommunications firms in Kenya and worldwide face challenges revolving around data privacy and security considerations. For instance, specific details of an individual's buying habits and lifestyle preferences are captured and analyzed through the firms' websites or by monitoring the social media. These details are all collected without individuals' absolute consent, leading to significant reservations about big data [3]. Privacy and data protection regulations are premised on individual control over information and on principles such as data minimization and purpose limitation. Yet, it is unclear that minimizing information collection is always a practical approach to data privacy [7].

II. PROBLEM STATEMENT

Although many studies have been carried out in the area of information security in the telecommunications sector in Kenya, there is lack of a structured framework for the effective management of bio data in these institutions. Serious incidents of privacy breaches can be damaging to the reputation of the telecommunications firm and therefore there is need for these institutions to implement effective information security management programs and to frequently monitor, review, maintain and improve them to safeguard information technology assets. One way of achieving this is to develop and implement personal data security and privacy framework. This study therefore sought to investigate privacy of bio-data held by telecommunications industry players and ultimately propose a framework for enhancing bio data privacy.

III. OBJECTIVE OF THE STUDY

The purpose of the study was to examine privacy issues concerning bio data in the telecommunications sector in Kenya and subsequently develop a framework to address the issues.

IV. RESEARCH QUESTION

What are the privacy issues affecting bio data obtained, processed and held by telecommunication firms in Kenya.

V. PERTINENT LITERATURE

In the past, the biggest privacy concerns have stemmed from citizens wanting to hide certain information from their governments. This is still a major issue in modern society, but as the power of corporations has grown, the bigger issue of consumer privacy has emerged. The Internet Age, which enables greater and faster access to consumer information and sophisticated online tools for exploitation, compounds this issue. This allows corporations to conceal online practices from less technologically savvy consumers. Consumer privacy has reached the point where it must be addressed, but in order to do so there must be a clear definition of privacy and clear goals of what privacy should accomplish [8]. Privacy is not simply a static concept, but instead it is an evolving concept whose content is often influenced by the political and technological features of the society's environment [9]. Many definitions of the concept abound in literature. This study adopts the view of privacy as freedom from epistemic interference that is achieved when there is a restriction on facts about someone that are unknown [10].

The study on privacy protection of personal data in general and bio-data in particular has attracted numerous researchers from different fields. In a study on data protection principles and cybercrime in Kenya, it was found that the Kenyan legal framework is dismally wanting when it comes to the protection individual privacy rights and rights

to personal information as enshrined in the dignitarian rights school of thought that all human beings are born free and equal in dignity and rights. Lack of protection of these rights has led to the increase in cyber crime and other related crimes that infringe on the privacy rights of individuals [11].

In a similar study but focusing on Small and Medium Enterprises (SMEs), it was established that the SMEs studied were highly reliant on Information Technology for their business operations hence the risk posed by failure of IT security was high. The study found that the major perceived and experienced threats to security were viruses and system users. The study also found that in the SMEs, there were some attempts at securing the IT assets though these efforts were largely uncoordinated [12].

Information security management in public universities has also attracted interest by scholars. In one study in Kenya, it was found that the information security control environment in public universities is inadequate to deal effectively with information security threats. According to the researcher, the main barriers to information security included enforcement of policies, lack of senior management support and lack of resources [13].

The literature review demonstrates that privacy and data protection has attracted research interest from the academic world. However, there are no studies expressly focusing on bio data privacy in the telecommunications industry in Kenya.

VI. THEORETICAL FRAMEWORK

This study is anchored on the Restricted Acess/Limited Control (RALC) theory of privacy [14]. The proponents of this theory outline three important elements of RALC. First, privacy is defined in terms of protection or limitation of access by others in the context of the situation. Second, an individual has normative privacy when there are explicit norms or laws protecting them and finally, policies provide individuals with the limited control necessary to manage their privacy. The RALC theory stresses the importance of setting up zones that enable individuals to limit or restrict others from accessing their personal information. It also recognizes the important role that individual control plays in privacy protection. The RALC theory requires us to review the context of the situation at hand. This begins with looking at the agents involved. In most cases, there is an individual subscriber who is being monitored and profiled by a telecommunications company. Other agents involved in our proposed framework include device manufacturers, communication service providers, third parties and telecommunication regulators. It is also important to note that the subscriber is often unaware of the information that is being tracked. Even though they have usually implicitly agreed to this, it is difficult to decipher what is actually being tracked without expertise. The situation can be summarized as a telecommunication company taking advantage of a subscriber's lack of knowledge and putting the information collected into other uses. In this situation, the subscriber's privacy is being violated rather than protected, and the actions of the companies responsible are rarely transparent due to the complexity of the tools being used. The

main issue here is information asymmetry whereby the telecommunication company knows more about what is being collected than the consumer. This asymmetry can be corrected by adopting the proposed bio-data protection framework which allows subscribers to give only necessary information and know how the information will be used [15].

Moreover, in the RALC framework, an individual enjoys some degree of control with respect to considerations involving choice, consent, and correction. For example, subscribers need some control in choosing which situations are and which are not acceptable to them with respect to the level of access granted to others. In managing their privacy, subscribers can also use the consent process. For example, they can waive their right to restrict others from access to certain kinds of information about them. The correction process also plays an important role in the management of privacy because it enables individuals to access their information with an ability to amend it if necessary. The proposed framework further ensures that the actions of the telecommunication companies and third parties would be transparent [16].

VII. METHODOLOGY

This study employed a descriptive survey design in which information was gathered through administration of questionnaires to a sample of respondents. The design adopted sought to describe the attributes of the larger population of telecommunication operatives drawn from the sample. The study relied solely on primary data collected using structured questionnaires distributed to 31 professionals in the area of information security management in the telecommunications sector. Participants were chosen through purposive sampling based on their lived experiences and specialized knowledge in data security. The questionnaires sought to obtain information pertaining to general information of the respondent and that of the firm, extent of bio data protection in the firm, registered threats and recommendations on data safety and security. It also contained the proposed bio data privacy framework for validation by respondents.

VIII. RESULTS AND DISCUSSIONS

This study endeavoured to develop a framework on bio-data privacy which can be used by the telecommunications sector to address the challenges of bio-data privacy in Kenya. The results of the study showed that telecommunication firms suffered bio data privacy threats to their systems. The results of the study revealed that majority of the organizations found the framework to provide a clear and systematic method for the protection of bio data privacy. Consequently, firms in telecommunications sector can adopt the proposed bio data privacy protection framework because it has been found to be clear and systematic, useful in practice and adaptable as well as customizable to different company settings. The developed framework and accompanying explanations are presented in the following figure.

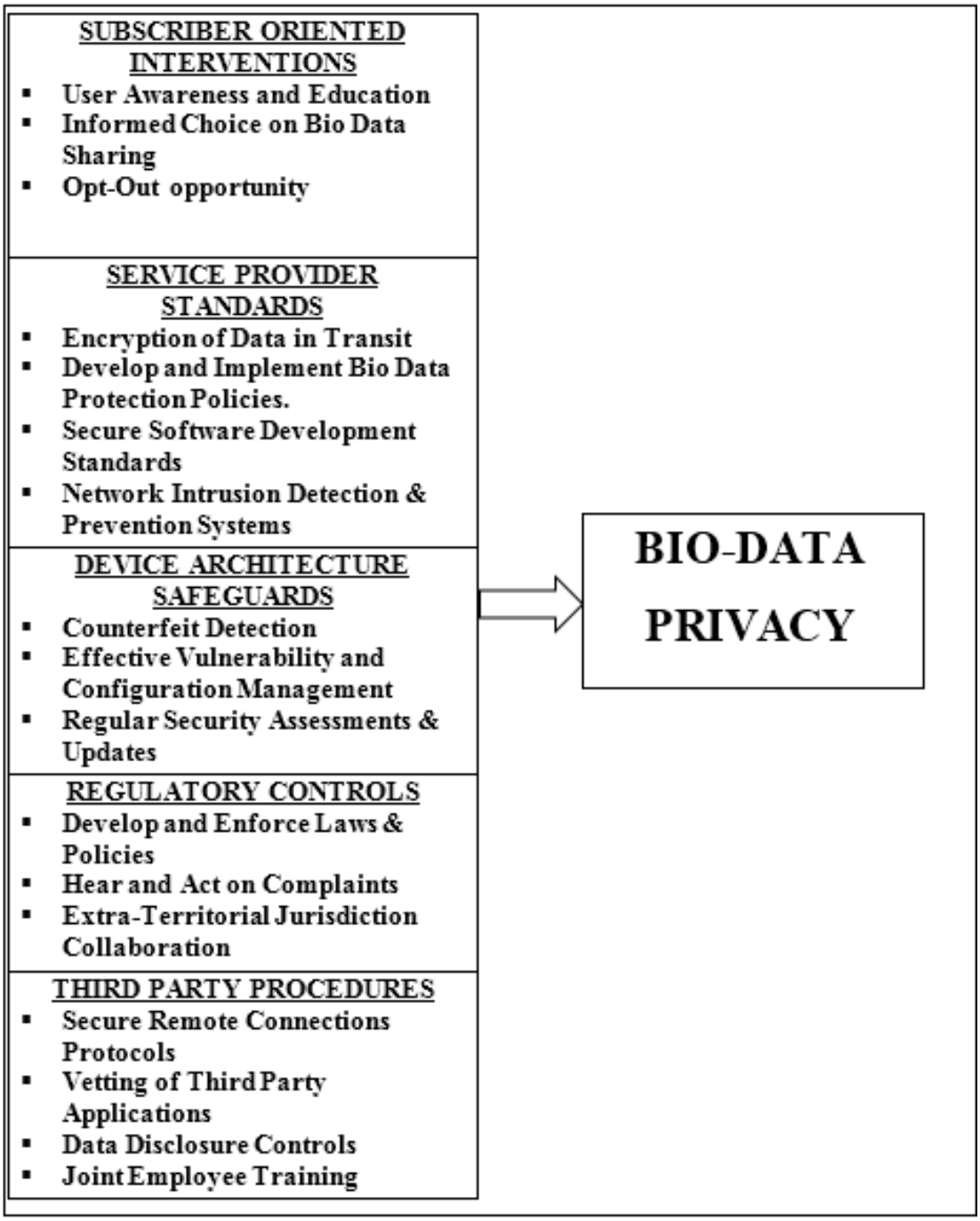

Figure 1: Telecommunications bio data privacy protection framework

Subscribers

These are the consumers of the telecommunications services. They provide bio data to the telecom firms with the hope that it will be used for the right purposes. Proposed solutions to protect their bio data include encryption of data in transit, secure software

development standards. Consumers should be able to make more informed choices about what information they share and with whom. Opt-out opportunities should be more clearly described and offered at a time when the consumer is making a decision about disclosing personal information.

Communication Service Providers (CSPs)

These are information technology professionals who play different roles in bio data processing, control and protection. The framework recommends the following remedies: clear data protection policies, multi-factor authentication, strong encryption of data at rest, network intrusion prevention systems, secure software development standards and vulnerability scanning of services. All in all, CSPs must inform subscribers of the purposes for which their personal data will be collected, used and disclosed prior to such collection, use or disclosure.

Device manufacturers

Device manufacturers make telecommunications equipment which is used by subscribers and CSPs. There is an increasing trend for manufacturers to offer products that 'just work' by making the configuration process as short as possible and relying on unnecessarily permissive default settings. Proposed solutions comprise the following: pay close attention to vulnerabilities in the network services of telecommunication equipment, establish effective vulnerability and configuration management processes. Also, regularly perform security assessments, including penetration testing for different types of attackers.

Third party

Third parties as those entities which are different to the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, but are authorized to process the data. The framework recommends the following solutions to forestall privacy threats: complete assimilation of the end user’s potential use into the company through joint employee training sessions, tightly monitored and fixed user lists, using secure remote connection protocols and applying extra layers of monitoring to these workstations will mitigate the possibility of external, unauthorized access and forming goal-specific access groups to these devices to ensure both domain-controller regulations and other agents can assist in identifying anomalies in real time.

Regulator

The regulatory authority is a statutory body responsible for the regulation of the electronic communications sector. The developed framework requires the regulator to enforce data protection laws at a national level, providing guidance on the

interpretation of those laws and oversight on bio data processing activities taking place within the territory.

IX. CONCLUSIONS

The results of the descriptive survey analyzed in this paper reveal that although telecommunications firms have adopted several bio data protection measures, these measures have not absolutely translated to bio data privacy. A significant number of organizations in telecommunications sector have not done enough to protect subscriber's bio data. We developed a framework which highlights the roles of key telecommunications actors in ensuring bio data privacy. The developed bio data privacy protection framework is clear, systematic, useful in practice and customizable to different organizational settings. We believe that the framework will be very helpful for policy planners and implementers in the ever growing telecommunications industry.

REFERENCES

[1] Wahab, S., *et al*., 2011, "The Influence of Perceived Privacy on Customer Loyalty in Mobile Phone Services: An Empirical Research in Jordan," International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011, pp. 1 – 5.

[2] Warren, S. and Brandeis, L., 1890, "The right to privacy," Harvard Law Review 4, pp. 193-220.

[3] Malala, J., 2013, "Consumer Protection for Mobile Payments in Kenya: an Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments," Kenya Bankers Association, Nairobi, pp. 23.

[4] Chua et al., 2015, "Conference Paper on the Implementation of the Privacy Protection Policy for Big Data Analytics: Challenges Faced in the Malaysian Telecommunications Industry," pp. 1- 10.

[5] Dirndorfer A. T. & Gardiner, G., 2014, "What Price Privacy in a Data-Intensive World?" In M. Kindling & E. Greifeneder (Eds.), Culture, Context, Computing: Proceedings of iConference 2014, pp. 1227–1230.

[6] Kobsa, A., 2007, "Privacy-Enhanced Web Personalization". In P. Brusilovski, A. Kobsa, & W. Nejdl (Eds.), The Adaptive Web: Methods and Strategies of Web Personalization, Springer, Berlin, pp. 628–670.

[7] Tene, O., & Polonetsky, J., 2013, "Big Data for All: Privacy and User Control in the age of Analytics," Northwestern Journal of Technology and Intellectual Property, 11, pp. 239–273.

[8] Confer, S. (n.d). A Socialist Theory of Privacy in the Internet Age: An Interdisciplinary Analysis. *Philologia* Volume: IX.

[9] Moor, J.H. (2006). Using genetic information while protecting the privacy of the soul. In: Tavani, H.T. (Ed.), *Ethics, Computing, and Genomics*, Jones and Bartlett, Sudbury, MA, pp. 109–119.

[10] Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology,* 1(1), 185–200.

[11] Mwangi, W.R., 2010, "Data Protection Principles and Cyber Crime in Kenya," Dissertation Submitted in Partial Fulfillment of the Requirements for the Master of Laws Degree to the Catholic University of Eastern Africa.

[12] Makumbi, L., Miriti, E.K., & Kahonge, A.M., 2012, "An Analysis of Information Technology (IT) Security Practices: a Case Study of Kenyan Small and Medium Enterprises (SMEs) in the Financial Sector," International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012, pp. 4.

[13] Kitheka, P.M., 2013, "Information Security Management Systems in Public Universities in Kenya: a Gap Analysis between Common Practices and Industry Best Practices," A Research Project Report Submitted in Partial Fulfillment of the Requirements for the award of Masters of Science Degree in Information Systems. University of Nairobi. Pp 82 -83.

[14] Tavani, H.T. and Moor, J.H. (2001). Privacy Protection, Control of Information, and Privacy Enhancing Technologies. *Computers and Society*, 31(1), 6–11.

[15] Tavani, H.T. (2007). Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology, 2nd edition. John Wiley & Sons, Hoboken, NJ.

[16] Himma, K.E. and Tavani, H.T. (2008) (eds.). *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Willey & Sons Inc.