

## ABSTRACT

Telecommunications are since long subject to privacy discussions, not so much for questions about the ringing phone but for the sensibility of the information that can be extracted from telephone services. It is against this backdrop that this study sought to examine privacy issues concerning bio-data in the telecommunications sector in Kenya and subsequently develop a framework to address the challenges. The objectives were to examine threats and evaluate measures in place for ensuring privacy of bio data in telecommunication firms; to develop a framework on bio-data privacy and adopt one that can be used by the telecommunications sector to address the challenges of bio-data privacy and to validate the developed bio data privacy protection framework. A descriptive survey targeting information security professionals and users of information systems was carried out. All Kenyan telecommunications firms were targeted from where the departments directly involved in data security were purposively selected. A total of thirty one (31) IT security professionals participated in this survey. A structured questionnaire was used for collecting primary data for the study. From the study, quantitative as well as qualitative data was gathered. The collected data was analysed thematically using the Statistical Package for Social Sciences (SPSS) version 21 to generate frequency tables and finally cumulative percentages which were thereafter tabulated and also presented in graphs and pie charts using Microsoft excel. The findings indicated that bio data privacy threats were rife in the telecommunication sector. The major bio-data privacy threats were computer viruses followed by data leakage. The other reported threats were denial of service attacks, software bugs, and spamming. The frequency of occurrence of the threats was reported to be rare. From the findings, training was the leading strategy for protecting bio data since majority of the respondents had received training in information security. A small numbers had not received any structured training on information security. In addressing the constraints and challenges faced by telecommunications firms, the findings assisted the researcher to develop a framework to be adopted by stake holders to ensure that there is privacy of customer's bio data. The proposed framework was reported by many respondents as being clear and systematic in the protection of bio data privacy. In conclusion, the study observes that bio data privacy threats are real in the ever growing and lucrative Kenyan telecommunications industry. It is recommended that telecommunication firms must identify and understand the privacy and security regulations that apply to the bio data they store, process, and transmit. They need also to implement a comprehensive bio data privacy protection framework like the one developed by the researcher.