Information
Impact

JOURNAL OF INFORMATION AND KNOWLEDGE MANAGEMENT
2024, VOL. 15, NO. 2, 45-58: ISSN: 2141-4297 (print) 2360-994X (online)
https://dx.doi.org/10.4314/iijikm.v15i2.4

To cite this article: Awuor, A. S, Okoth, P. & Kwanya, T. (2024) Navigating ethical dilemmas while transforming information services in the global age. Information Impact: *Journal of Information and Knowledge Management*, 15:2, 45-58, DOI https://dx.doi.org/10.4314/iijikm.v15i2.4

To link to this article: https://dx.doi.org/10.4314/iijikm.v15i2.4

Navigating Ethical Dilemmas while Transforming Information Services in the Global Age

[1]Afline Susan Awuor
[1]Paul Okoth
[2]Tom Kwanya

[1]Tangaza University College
[2]The Technical University of Kenya

Abstract

The digital age has transformed information services. Individuals and organisations create, access, and engage with information on a previously inconceivable scale. This digital landscape has ushered in novel and pressing ethical concerns. Issues surrounding data privacy, intellectual property rights, responsible use of technology, and the ethical delivery of information services have taken the centre stage. There is a need to ensure that information services are ethically sound and genuinely user-centric, placing user rights and ethical considerations at the heart of service design and delivery. This paper identifies emerging ethical challenges information services face in the digital era, examines the technological advancements and innovations that have given rise to the ethical challenges in the provision of information services, analyses the existing legal and regulatory frameworks that pertain to information services in the digital landscape, and reviews case studies and best practices in information services that have successfully addressed emerging ethical challenges. The study employed a qualitative research approach. Data was collected by reviewing current literature, legislation and regulations, and ethical guidelines to understand the recommended ethical standards for information services in the digital era. The findings revealed that technological advancements and innovations enable better content creation, delivery, data storage, and efficient information retrieval. However, they also introduce ethical challenges related to bias, privacy, security, and responsible use of information and technology. The study findings can contribute to a more responsible and ethical information service, ensure user satisfaction and legal compliance, and promote innovation and adaptation. The results can also create public awareness and inform policy development that addresses ethical challenges.

Keywords

Ethical dilemmas, digital age, digital landscape, intellectual property rights, data privacy

CONTACT TOM Kwanya@ tkwanya@tukenya.ac.ke

Introduction

In today's interconnected world, information has become the new currency. Technological advancements, like the Internet and social media, have changed how information is created, accessed, shared, and stored. Technological advancements have enriched the information landscape. However, they have also ushered in ethical concerns involving responsible use of technology, data privacy, and intellectual property concerns such as copyright infringement, patent violations, and plagiarism. For instance, Chepchirchir et al. (2019) argue that the management of intellectual property rights in digital contexts is increasingly becoming complex since digitisation increases the vulnerability of digital works and exposes them to violation. The growing ubiquity of autonomous machines, such as collaborative robots, has further exacerbated the ethical complexities of the modern information universe (Kwanya, 2023). Therefore, new ethical challenges about information service delivery and use have emerged. Mittelstadt and Floridi (2016) opined that the complex interplay between technological advancement and responsible use of technology calls for a careful examination of digital interactions. Kwanya (2021) explained that more sophisticated ethical issues have surfaced as people humanise machines to the extent that they regard them as colleagues. Kibe et al. (2023) echoed the same concern and pointed out that the Fourth Industrial Revolution (4IR) will permanently transform how people seek, use and share information thereby raising unforeseen ethical dilemmas.

Laws, rules, and regulations govern how information is created, used, and shared in the digital landscape. These laws form the backbone of ethical practices in information services, ensuring individuals navigate the digital landscape more transparently and accountably. Awojobi and Landry (2023) added that these regulations ensure that non-compliance has consequences, including levies and fines. They further reckon that the regulations often lag behind technological advancement thus limiting their practical application. Individual countries have laws, rules, and regulations to ensure information and technology are used justly, ethically, and responsibly (Kogos & Kwanya, 2023). These guidelines help maintain a balance between technological advancement, privacy, and data security. However, their effectiveness and efficiency vary from country to country and remains a subject of present discourse.

Literature review

The literature review explored existing literature, ethical guidelines and legislation on ethical challenges and standards for information services in the digital age. This included reviewing books, scholarly articles, legislation and regulatory frameworks, ethical guidelines, and other relevant sources. The aim was to understand and provide insights into the ethical standards for information services in the digital era.

Technological advancements and the Internet have transformed how information is created, accessed, used, and shared. This transformation is characterised by the use of digital tools to enhance accessibility, improve search accuracy, and manage vast information sources and resources. This has given rise to ethical challenges, with information professionals bearing ethical responsibility to protect user data and privacy. Mittelstadt and Floridi (2016) argued that personal data has become a commodity, causing concerns regarding user consent, misuse of information, and unauthorised access.

According to Dijk and Hacker (2000), various barriers make access to technology and the Internet more difficult for specific populations than others, raising ethical concerns about equitable access to information services. Despite strides in Internet connectivity and rural electrification in Kenya, a digital divide still exists in the rural areas and among low-income earners. Lusweti and Omieno (2023) averred that a digital divide does exist in Kenya, mostly among people living with disabilities, the elderly, those with low literacy levels, low-income earners and the unemployed. They further noted that frequent power outrages across the nation, particularly in the rural areas, and socioeconomic factors have resulted in these areas lagging in technology and innovation.

The digital era has witnessed the emergence of hyper-realistic artificial intelligence-generated videos and audio that spread false or misleading information in social media. This is particularly true in the context of Kenya during the election period. Wardle and Derakhshan (2017) raised concerns about mis-, dis-, and mal-information in social media. They examined information disorder, addressing challenges that influence how people consume and interact with information in the digital age, such as filter bubbles (getting stuck in your personalised online space and only getting information that you like or aligns with your opinions) and echo chambers (a space or environment that reflects of reinforces pre-existing opinions) emphasising that information professionals are obligated to prevent the spread of false information.

The advancement of mobile technology and devices brings forth several advantages, including being mobile-centric and using the Internet to expand information access, self-expression, news, and entertainment. However, this has given rise to ethical challenges such as hacking, information privacy, and data privacy, among others (Crotty, 2017; Donner & Shikoh, 2009). Mobile applications such as M-Pesa, the world's leading mobile money service company by Safaricom, a telecommunications company in Kenya, allow for making payments, saving, sending, and receiving money. M-Pesa provides access to financial services but raises ethical concerns about data privacy, financial inclusion and equity. Similarly, the use of technology in managing medical records to improve efficiency and efficacy also increases risks to data security and privacy of health information (Sajjad & Shahid, 2016). Closed-circuit television (CCTV) technology is being used as security measures for homes, companies, and traffic for mass surveillance to monitor and prevent crime. CCTV technology operates in various settings, public and secret, and has gained global ramifications on individual privacy. Chen (2017) affirmed that using CCTV technology has raised concerns over the balance between intelligence, privacy rights, consent, and transparency.

Legal and regulatory frameworks govern information services in the digital landscape. These legal and regulatory frameworks comprise an expansive range of policies, laws and regulations governing how information is created, stored, and shared. These frameworks aim to have a fair operational parameter in the digital landscape. Each nation has its own legal and regulatory framework of information services that cover intellectual property, data protection and privacy, and responsible use of technology. Data protection and privacy framework safeguards personal and public data, indicating how they can be stored and shared and who has access to it. It also states the responsibilities of data processors and controllers (Jerameel & Kibet, 2022).

The Communications Authority of Kenya (CAK) regulates the country's Information and Communications Technologies industry. CAK outlines roles aimed at protecting digital infrastructure, e-commerce, consumer rights, poster services, telecommunications, and broadcasting in the ICT industry (United Nations Conference on Trade and Development, 2022; Wanyama, 2015). Kenya Information and Communications (Cybersecurity) Regulations, a regulation by the Communications Authority of Kenya, provides measures on cybersecurity for reporting incidents and information service providers. Notable studies by various researchers, such as Alkhurayyif (2023), Leith (2021), Maina (2020), and Regulation (2018), showcase successful techniques for addressing ethical challenges.

Leading technological companies have initiated measures to ensure safety in digital spaces. One is Google's Project Zero, an initiative to hunt for a zero-day flaw in Google products, cloud services, hardware, and software. It then gives vendors 90 days to fix the issue. Project Zero ensures that people have a safe and open Internet. Another initiative is the General Data Protection Regulation (GDPR), a regulation implemented by the European Union to protect data. It gives ordinary people unprecedented control over the data companies hold on them, such as names, phone numbers, emails, social media handles, gender, and race. All organisations except hospitals, government agencies, and journalists must have a lawful reason to hold anyone's data or individual consent and prove that the data is safe.

Other initiatives target web browsers, which are the gateway to the digital ecosystem. These web browsers allow people to connect, create, access, and share information. One such web browser that stands out is Mozilla Firefox, an open-source project funded by the Mozilla Foundation, with the latest version being version 120. Mozilla Firefox is a power-centric browser that provides features such as private browsing, AD blocking, fingerprint blocking, and enhanced tracking protection. Mozilla, therefore, allows for the customisation of privacy preferences and the blocking of trackers.

Despite the local and international initiatives to make digital spaces safe, personal data security vulnerabilities still abound. Therefore, threats to data privacy, intellectual property rights, responsible use of technology, and the ethical delivery of information services persist. Therefore, there is a need to ensure that information services are ethically sound and genuinely user-centric, placing user rights and ethical considerations at the heart of service design and delivery. This paper explores how digital transformation has reshaped the ethical landscape of information services. It also highlights the ethical intricacies that have emerged in the digital age, focusing on data privacy, intellectual property, and responsible technology use. The specific objectives of the study are to identify emerging ethical challenges information services face in the digital era, examine the technological advancements and innovations that have given rise to the ethical challenges in the provision of information services, analyse the existing legal and regulatory frameworks that pertain to information services in the digital landscape, and review case studies and best practices in information services that have successfully addressed emerging ethical challenges.

Methodology

This study used a qualitative research approach involving collecting qualitative data through document analysis and reviewing existing literature on the topic. The literature included books, scholarly articles, legislation and regulations, ethical guidelines, and other relevant information sources. The review aimed to understand the recommended ethical standards for information services in the digital era. The literature review provided insights from previous research, while the document analysis focused on extracting specific legal information related to ethical information services. Literature sources were identified and retrieved from online databases, including EBSCO, JSTOR, ERIC, Google Scholar and ACM Digital Library. The information sources were identified using appropriate search terms and phrases. These included "technological advancements AND ethical challenges", "user experience dilemmas", "ethical considerations in information access", "information delivery ethics", "information accessibility ethics", "user interface ethics", "information dissemination ethics", "legal and regulatory frameworks AND information services AND digital landscape", "ethical dilemmas in information delivery in the digital era" and "user navigation dilemmas". The analysis included papers directly addressing ethical issues on information delivery, navigation, or access; peer-reviewed journal articles, conference papers, and books; literature published within the past 13 years; and papers available in full text. Materials not directly addressing ethical dilemmas in information delivery, navigation, or access; non-peer-reviewed literature; and literature older than 13 years were excluded. The collected data was analysed thematically.

Findings and discussions

The revelations from the literature review and document analysis show an insight into the varied ethical challenges encountered in the evolving landscape of information services. The findings presented in this section summarise the recurring themes and critical considerations derived from the literature review into ethical dilemmas in information services within the digital age.

Emerging ethical challenges information services face in the digital era

The research identified significant concerns regarding data privacy, protection, and unauthorised access to personal data. With the proliferation of data-driven technologies and digital platforms, ensuring data privacy techniques and safeguarding personal information emerged as a paramount ethical imperative (Papaioannou et al., 2016). There have been cases of data breaches and surveillance of personal information. The Cambridge Analytica scandal saw Facebook users' data harvested for political profiling without proper authorisation, revealing significant data privacy and protection concerns.

There were also notable ethical concerns in areas such as Artificial Intelligence, cyber security threats, bias, vulnerabilities, and automation in information services. Research revealed biases and threats brought about by Artificial Intelligence. Aljaidi et al. (2022) mentioned the WannaCry attack. WannaCry exploited vulnerabilities in healthcare institutions using computers operating Microsoft Windows. User data was held hostage, and Bitcoin ransom was demanded. Resnik (2015) revealed bias in recruiting Artificial Intelligence platforms. He noted that Artificial Intelligence platforms with biased algorithms raise ethical concerns about transparency, unintended consequences, and fairness in automated decision-making.

There is a need to enhance digital resilience in order to curb the growing cybersecurity threats and ransomware attacks. This can be achieved by addressing digital divides, ensuring equitable access to information services, and fostering inclusive digital ecosystems (Kreps et al., 2021). Implementing ethical artificial intelligence standards for fairness, transparency, and accountability is crucial. General Data Protection Regulation (GDPR) by the European Union provides a framework that aims to navigate ethical challenges by safeguarding data and ensuring user rights and organisational accountability (Creswell & Creswell, 2018).

Technological advancements and innovations that have given rise to the ethical challenges

Findings revealed the dual role of technological advancements and innovations. Technology facilitates progress by streamlining and automating information services tasks but is also a source of concern. Artificial Intelligence (AI), the Internet of Things (IoT), and Big data analysis emerged as transformative forces. Gazis et al. (2015) agreed that Artificial Intelligence, the Internet of Things (IoT), and Big Data analytics have shaped how information is created, organised and shared. Big Data analytics uncovers patterns and trends that aid in making informed decisions, while AI-driven algorithms and devices aid in personalising and tailoring content to an individual's preference. Njeru (2014) is of the contrary opinion that the complexity of technology and technological advancements and innovations are likely to increase virtual or social media interaction and cause an erosion of genuine human interactions. Kaur and Preeti (2010) raised concern about the speed at which technology advances, claiming it might outpace our ability to use it effectively.

While these technological advancements and innovations enable content creation, delivery, data storage, and efficient retrieval of information, they also introduce ethical challenges related to bias, privacy, security, and responsible use of information and technology. Zostant and Chataut (2023), Biros (2020) and Talwar (2019) agree and point out that ethical challenges in information services lie between harnessing technological advancement and protecting individual rights. They mentioned digital divide, data integrity and confidentiality, discrimination due to AI algorithm bias, ownership and data control issues as some ethical challenges.

Legal and regulatory frameworks that pertain to information services

The findings revealed a foundational document the United Nations General Assembly endorsed, the Universal Declaration of Human Rights (UDHR). UDHR is a framework that influences and guides how laws and policies are developed to ensure that fundamental human rights are universally protected (Howie, 2018). Other associations, such as the International Federation of Library Associations and Institutions (IFLA) and the American Library Association (ALA), operate in different scopes but guide the operations of libraries and librarians, focusing on access to information, privacy and intellectual freedom.

In Kenya, legal frameworks governing information services include regulations, statutes, and constitutional provisions. Kenya’s Constitution (2010) offers comprehensive guidelines that protect the rights and freedoms of its citizens. The

Constitution has provisions that directly or indirectly impact information services. Hereunder are the provisions that directly impact information services.

Kenya's Data Protection Act (2019) ensures that individuals' rights and privacy are respected. The Act outlines how data should be processed, rights to data subjects, cross-border data transfers, and penalties for non-compliance. The Copyright Act (2001) has been shaped by international treaties and agreements such as the Cotonou Agreement, the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement, the African Growth and Opportunity Act (AGOA), and the World Intellectual Property Organization (WIPO) Copyright Treaty (Olaka & Adkins, 2012). The Copyright Act (2001) protects musical, sound recordings, artistic works, literary works, cinematography and broadcasts. It gives guidelines on fair dealings, exceptions and limitations, remedies and enforcement, and rights to copyright owners. Access to Information Act 2016 article 35 addresses access to information held by the government and non-state entities. The Act emphasises the correction of untrue information, accuracy, and transparency (Mathangani & Otike, 2017).

These provisions may not be sufficient since their sufficiency depends on an entity's expectations and needs. Under the Copyright Act (2001), musical and sound recording works face the challenges of globalisation (Mungai et al., 2020).

Cases of digital data breaches

The Internet has ushered in an environment where individual or organisational data is created, managed, and stored in large quantities on cloud platforms and software applications. Due to software applications' vulnerability, these data can be easily accessed and shared, making them targets for cybercriminals. The findings highlighted cases where organisations faced and addressed ethical challenges in their information services practices.

Equifax, an agency in the United States of America whose primary role is to collect, organise and report on individual credit-related data such as credit history, outstanding debts, payment plans, and generating credit scores, suffered a data breach in 2017. Equifax failed to secure individual's data, leaving the system vulnerable to attack. Therefore, Equifax had to compensate those affected during the attack and put measures such as regular security audits in place to avoid similar attacks (Gaglione, 2019; Robbins & Sechooler, 2018).

Uber is a taxi company that hires drivers to use their cars and offer car services to customers on short notice. The driver and the passenger need the Uber App to use the service. Uber's system was breached in 2016, and data of millions of passengers and drivers, such as email addresses, names, and telephone numbers, were exposed.

Uber fired employees who tried to cover up the data breach and paid fines to regulatory bodies. Uber has since enhanced their security measures (Choi, 2021; McGovern, 2024; Robbins & Sechooler, 2018).

Google Street View is an app featured on Google Earth and Google Maps that visually represents the surroundings of different parts of the world. In 2010, Google Street View cars unintentionally collected data from WIFIs that were not adequately secured. Google Street View cars collected information such as emails and passwords without the consent of the users. After an outcry from the public, Google apologised, pledged to delete all the data collected unscrupulously, paid fines imposed by the regulatory authorities, and put up contingencies to avoid similar occurrences and ensure data privacy (Burdon & McKillop, 2014; Gallo & Houssain, 2020).

Facebook is an online social media platform that allows individuals and companies to post status updates, send messages, and share videos and photographs. In 2018, Facebook's CEO, Mark Zuckerberg, was accused of granting over 150 tech companies access to users' information. This revelation sparked a public outcry that led to scrutiny from lawmakers and regulatory bodies. Facebook's CEO issued a public apology, acknowledging the platform's responsibility for the incident, paid fines and other settlements to regulatory bodies, and has since introduced features for more privacy of user information (Trautman, 2020; Tuttle, 2018).

In Kenya, Nzuva (2019) reports that commercial banks have experienced numerous cases of data breaches due to inadequate risk management strategies. Similarly, Njeri (2014) pointed out that there has been an upsurge of financial transaction frauds in the country leading to massive losses to financial institutions and their customers. Kigen et al. (2015) argued that since many incidents go unreported, the value of individual and institutional losses arising from data breaches in Kenya remains unknown though perceived as significant.

Conclusion

This paper explores ethical dilemmas faced by information services in the digital age. The digital age is characterised by technological advancement and innovations. This integration of technology into information services brings about opportunities as well as challenges. Technology integration in information services has improved the speed at which information is created, organised, stored and shared. However, it has raised ethical concerns such as algorithm bias, digital divide, data privacy, and misinformation. Ethical considerations are therefore vital in the creation, use, organisation and management of information services to ensure protection and reliability. This paper recognises that there are legal frameworks that govern information services in Kenya, but they are deemed insufficient since their sufficiency depends on society's needs at a given time. It concludes that there is a need for the available legal frameworks to evolve to address the emerging ethical dilemmas fully.

Recommendations

The study recommends measures to aid in navigating ethical dilemmas inherent in information services:

- Employ a heightened public awareness campaign and advocate for the need to provide sufficient information on data. Organisations should provide information that is easy to access and understand, detailing what kind of data is needed, why they need it, and how it will be used.
- Organisations handling personal data should foster a culture of accountability and transparency. They should ensure that they have clear guidelines on how to respond to ethical incidents and hold those who are non-compliant responsible for ethical lapses.
- Empowering users to make informed decisions is necessary. Organisations should prepare and make available informed consent forms. The consent processes should be easy to read and understand and state why the data is needed and what it will be used for.
- Continuous training and workshops should be provided for professionals involved with information services. This will ensure they have an environment to discuss emerging trends and learn how to address ethical challenges.
- Engage stakeholders and champion regular reviews of the legal frameworks about information services, ensuring that the legal updates cater to diverse perspectives.

References

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S., Khalid, M., & Al-Gumaei, Y. A. (2022, November). NHS WannaCry Ransomware Attack: Technical Explanation of The Vulnerability, Exploitation, and Countermeasures. In *2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)* (pp. 1-6). IEEE.

Alkhurayyif, Y. (2023). Users' information security awareness of home closed-circuit television surveillance. *Journal of Information Security and Cybercrimes Research*, *6*(1), 12–23. https://doi.org/10.26735/VFKO2846

Awojobi, B., & Landry, B. J. (2023). Examining data privacy through the lens of government regulations. In *Effective Cybersecurity Operations for Enterprise-Wide* (pp. 80–94). IGI Global. https://doi.org/10.4018/978-1-6684-9018-1.ch003

Biros, D. (2020). The challenges of new information technology are security, privacy, and ethics. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2020*(2), 1. https://doi.org/10.17705/3jmwa.000057

Burdon, M., & McKillop, A. (2014). The Google Street View Wi-Fi scandal and its repercussions for privacy regulation. *Monash University Law Review*, *39*(3), 702–738. https://doi.org/10.3316/informit.376209506308923

Chen, K. (2017). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state. *Intelligence and National Security*, *32*(6), 868–871. https://doi.org/10.1080/02684527.2016.1254142

Chepchirchir, S., Limo, J., & Kwanya, T. (2020). Intellectual property rights in digital libraries: Status, interventions, challenges, and opportunities for academic libraries in Kenya. *International Journal of Information Studies & Libraries* 5 (2) 2020, 93-102

Choi, Y. B. (2021). Organisational cyber data breach analysis of Facebook, Equifax, and Uber cases. *International Journal of Cyber Research and Education (IJCRE)*, *3*(1), 58–64. https://doi.org/10.4018/IJCRE.2021010106

Creswell, J. W., & Creswell, D. J. (2018). *Research design: Qualitative, quantitative and mixed methods approaches* (5th ed.). SAGE PublicationsSage CA: Los Angeles, CA.

Crotty, B. H. (2017). Considerations and challenges in information and communication technology. In *Ethical Considerations and Challenges in Geriatrics* (pp. 147–156). https://doi.org/10.1007/978-3-319-44084-2_13

Dijk, J. van, & Hacker, K. L. (2000). *Digital Democracy : Issues of Theory and Practice*. SAGE Publications Ltd.

Donner, J., & Shikoh, G. (2009). New paths: exploring mobile-centric internet use in South Africa. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 761–770.

Gaglione, G. S. J. (2019). The Equifax data breach: An opportunity to improve consumer protection and cybersecurity efforts in America. *Buffalo Law Review*, *67*(4), 1133. https://heinonline.org/HOL/Page?handle=hein.journals/buflr67&id=1171&div=&collection=

Gallo, P., & Houssain, K. (2020). On Privacy Issues with Google Street View. SDL Rev. *SDL Rev.*, *65*, 608.

Gazis, V., Gortz, M., Huber, M., Leonardi, A., Mathioudakis, K., Wiesmaier, A., Zeiger, F., & Vasilomanolakis, E. (2015). A survey of technologies for the Internet Internet of Things. *IWCMC 2015 - 11th International Wireless Communications and Mobile Computing Conference*, 1090–1095. https://doi.org/10.1109/IWCMC.2015.7289234

Howie, E. (2018). Protecting the human right to freedom of expression in international law. *International Journal of Speech-Language Pathology*, *20*(1), 12–15. https://doi.org/10.1080/17549507.2018.1392612

Jerameel, K., & Kibet, B. (2022). Defining Data Protection in Kenya: Challenges, Perspectives and Opportunities. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.4270712

Kaur, H., & Preeti, S. (2010). Role of technological innovations in improving library services. *International Journal of Library and Information Science*, *2*(1), 11–16.

Kibe, L., Kwanya, T., & Nyagowa, H. (2023). Harnessing fourth industrial revolution (4IR) technologies for sustainable development in Africa: a meta-analysis. *Technological Sustainability*, *2*(3), 244-258.

Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., & Ndegwa, D. (2015). & Shitanda, S.(2015). *Kenya Cyber Security Report 2015*.

Kogos, A. C., & Kwanya, T. (2023). Public access to information and open governance in Kenya. Data Science & Informetrics, 3(4), 22-33.

Kreps, D., Moira, de R., Don, G., & Havey, M. (2021). *IFIP Code of Ethics and Professional Conduct*. https://doi.org/10.52545/2-2

Kwanya, T. (2023). Working with robots as colleagues: Kenyan perspectives of ethical concerns on possible integration of Co-bots in workplaces. In *Responsible AI in Africa: Challenges and Opportunities* (pp. 65-99). Cham: Springer International Publishing.

Kwanya, T. (2021). Perception of robots in Kenya's infosphere: Tools or colleagues? In: D.N. Ocholla, N.D. Evans & J. Britz (eds.), *Information knowledge and technology for development in Africa*, pp. 37–56, AOSIS, Cape Town. https://doi.org/10.4102/aosis.2021.BK262.03

Leith, D. J. (2021). Web browser privacy: What do browsers say when they phone home? *IEEE Access*, p. *9*, 41615–41627. https://doi.org/10.1109/ACCESS.2021.3065243

Lusweti, S. W., & Omieno, K. K. (2023). Using I-Hubs for Bridging The Gap of Digital Divide in Rural Kenya. *Buana Information Technology and Computer Sciences (BIT and CS)*, *4*(2), 54–62. https://doi.org/10.36805/BIT-CS.V4I2.5165

Maina, S. K. (2020). *A Model for identifying vulnerabilities on critical infrastructures: Case of cyber threats in Kenya*. Strathmore University.

Mathangani, S. W., & Otike, J. (2017). The legal implications of providing information services in PUL in Kenya. *Journal for Library Culture*, *5*(1), 16–31.

McGovern, V. (2024). *Uber: Cyber breaches. In Sage Business Cases.* SAGE Publications. https://doi.org/10.4135/9781071939994

Mittelstadt, B. D., & Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Law, Governance and Technology Series*, *29*, 445–480. https://doi.org/10.1007/978-3-319-33525-4_19/COVER

Mungai, M. W., Dorvlo, S. S., Nuwagirya, A., & Holmner, M. (2020). Influence of copyright exceptions and limitations on access to information in Kenya, Ghana and Uganda libraries. *Library Management*, *41*(6–7), 565–577.

https://doi.org/10.1108/LM-03-2020-0052/FULL/PDF

Njeri, W. (2014). *Upsurge of customers' transactions frauds in Kenya A case of Kenyan financial institutions* (Doctoral dissertation, United States International University Africa). http://erepo.usiu.ac.ke/bitstream/handle/11732/40/Njeri.pdf

Njeru, P. W. (2014). *Challenging the innovation paradigm as a means to technological advancement and economic development*.

Nzuva, S. (2019). Enhancing Data Breach Risk Management: A Case Study of Kenyan Commercial Banks. *Constitution*, *47*, 48.

Olaka, M. W., & Adkins, D. (2012). Exploring copyright knowledge in relation to experience and education level among academic librarians in Kenya. *International Information & Library Review*, *44*(1), 40–51. https://doi.org/10.1016/j.iilr.2012.01.005

Papaioannou, D., Sutton, A., & Andrew, B. (2016). *Systematic approaches to a successful literature review*. Sage. https://www.researchgate.net/profile/Andrew-Booth-2/publication/235930866_Systematic_Approaches_to_a_Successful_Literature_Review/links/5da06c7f45851553ff8705fa/Systematic-Approaches-to-a-Successful-Literature-Review.pdf

Resnik, D. B. (2015). *What is Ethics in Research, Why Is It Important*? https://www.niehs.nih.gov/research/resources/bioethics/whatis/index.cfm

Robbins, J. M., & Sechooler, A. M. (2018). Once More unto the Breach: What the Equifax and Uber Data Breaches Reveal about the Intersection of Information Security and the Enforcement of Securities Laws. *Criminal Justice*, *33*(4). https://heinonline.org/HOL/Page?handle=hein.journals/cjust33&id=6&div=&collection=

Sajjad, U. U., & Shahid, S. (2016). Baby+ is a mobile application to support pregnant women in Pakistan. *Proceedings of the 18th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, pp. 667–674. https://doi.org/10.1145/2957265.2961856

Talwar, R. (2019). Information technology and ethical issues. *International Journal of Computer Applications*, *178*(8), 34–35. https://doi.org/10.5120/ijca2019918784

Trautman, L. J. (2020). Governance of the Facebook privacy crisis. *Pittsburgh Journal of Technology Law & Policy*, *20*(1). https://doi.org/10.5195/TLP.2020.234

Tuttle, H. (2018). Facebook scandal raises data privacy concerns. *Risk Management*, *65*(5), 6–9. https://go.gale.com/ps/i.do?p=AONE&sw=w&issn=00355593&v=2.1&it=r&id=GALE%7CA538250056&sid=googleScholar&linkaccess=fulltext

United Nations Conference on Trade and Development. (2022). Legal and regulatory frameworks. In *Kenya eTrade Readiness Assessment* (pp. 42–50). https://doi.org/10.18356/9789210018630c011

Wanyama, L. L. (2015). Media control in Kenya: The state of broadcasting under the new Kenya Information and Communication Act of 2013. *New Media and Mass Communication*, *33*, 17–22. https://core.ac.uk/download/pdf/234652651.pdf

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27).

Zostant, M., & Chataut, R. (2023). Privacy in computer ethics: Navigating the digital age. *Computer Science and Information Technologies*, *4*(2), 183–190. https://doi.org/10.11591/csit.v4i2.p183-190