Navigating the Digital Abyss: A Conceptual Exploration of Internet Privacy, Personal Data Safety, and the Path Forward

[1]Prof. Ogochukwu, C. Ekwenchi & [2]Shadrach Idi

[1]Department of Mass Communication, Nnamdi Azikiwe University Awka
[2]Department of Mass Communication, Taraba State University, Jalingo
Email: shadrachidi@gmail.com

Abstract

As the Internet becomes increasingly integrated into daily life, the profound implications of privacy infringement and personal data vulnerability have come to the forefront of societal concerns. This study aims to unravel the multifaceted dimensions of internet privacy and data security. The research method used is a qualitative approach based on a narrative synthesis design. The sources of data include journals, books, and special reports by media, agencies, and the government on the subject matter. The study dissects the various techniques of data collection and data privacy infringement on the Internet by both cyber criminals and corporate entities, unravelling the intricacies of surveillance capitalism and its implications for individual rights and well-being. Furthermore, the study sheds light on the challenges of cyber protection in Nigeria and calls for a holistic approach to safeguarding internet privacy and personal data safety. It proposes a comprehensive framework that encompasses technological innovation, robust legislation, and user empowerment as integral components of fortifying digital privacy.

Keywords: Internet, Privacy, Personal, Data, Cyber, Safety,

Introduction

The Internet has become a necessary aspect of modern life. It is like the oxygen we take, without which many people and organizations might not survive because their daily lives ultimately depend on the Internet. For many individuals, the Internet remains the primary channel of communication, commerce, learning, news access, entertainment, and leisure, among others. Most organizations have integrated their operations with the Internet (PEW, 2018). For instance, schools provide an online learning experience, and many business organizations create digital ecosystems where they hold meetings, staff work from any location, and they reach their target audience. Religious organisations, like churches and mosques, were not left out. Several of these groups have created online platforms where their members can connect to the Internet for their live services.

In another dimension, the Internet has birthed several digital service providers and web-based companies such as e-banks and loan platforms. It seems no aspect of human life is without the impact of the Internet. Consequently, the adoption of the Internet and digital devices like smartphones has been massive globally. According to reports, 64.6% of people worldwide use the Internet (Statista, 2023). There is no doubt that the Internet has impacted our world positively in diverse ways. It has eased human life, brought speed to service delivery and access to information, created job opportunities, and connected local organisations or businesses to the global market. However, the Internet and new media use have led to profound concerns, particularly as it relates to the protection of individual privacy and personal data safety in the vast landscape of cyberspace. This is so because as individuals and organisations engage the Internet, online platforms collect, store, and utilise their personal data, such as name, address, search history, tweets, pictures, likes, and dislikes, among other sensitive data **(**Brynjolfsson, & McAfee, 2014). The information is

processed to form profiles of the users, which are further used for marketing, policies, and decision-making by different bodies, often without the knowledge or understanding of the Internet consumers.

Digital data collection has become a major sector in today's economy. Today, many organisations and governments depend on the data profiles of their citizens; therefore, big tech companies like Google, Facebook, and Amazon, among others, have primarily turned to digital data merchants. They have developed different intrusive systems with which they wish to mine users' data and monetize the data for governments and organisations in need of them. This phenomenon has raised critical questions about privacy infringement, data breaches, and the ethical use of information (Eddy, 2018). Similarly, Internet users are increasingly experiencing threats to online safety and cyber security and are becoming more concerned with e-crime, especially identity theft and financial scams (Alkhalil, Hewage, Nawaf, & Khan, 2021). Many people and organisations have experienced financial scams. The Centre for Strategic and International Studies (CSIS) reported that every year, a financial loss of 445 billion dollars in the world economy is recorded due to cybercrime **(***Daily Amar Desh*, 2014). In Nigeria today, online scams known as yahoo-yahoo are high, and many young people have made it their occupation. They spend enormous time on the Internet syphoning personal data of users and using the same to defraud the user or his or her networks.

Considering the increasing cases of data privacy breaches and cybercrimes, there has been a growing demand for cyber safety and cyber education around the world. Regional and national governments have established laws to safeguard the privacy and safety of Internet users in their territories. Popular among these laws are the General Data Protection Regulation (GDPR) by the European Union (Sobolewski, Mazur, & Paliski, 2017), the Cyber Security Framework by the United States National Institute of Science and Technology (NIST) (NIST, 2018), the African Union Convention on Cyber Security and Personal Data Protection by the African Union (AU) (Internet Society and the Commission of the African Union, 2018), and the National Data Protection Regulations (NDPR) of Nigeria (Odufuwa, 2021). In addition to policies and legislation, there has been an increasing social campaign intended to create awareness about cyber risks and educate and equip users with the skills and motivation to adopt Internet protection strategies. Furthermore, the issue of data privacy protection and risks is rapidly gaining attention in scholarship across different fields. Based on the aforementioned, the current paper is designed to shed light on the phenomenon of digital data risks and ways Internet users can protect themselves. This is important considering the fact that digital data breaches and cyber-attacks are complex and dynamic; hence, the users need to be adequately informed regarding the trend of breaches and attacks on the digital ecosystem. The study sought to contribute to the ongoing discourse surrounding internet privacy and personal data safety, providing valuable insights and recommendations for various stakeholders involved in shaping policies, technologies, and user behaviour in the digital realm.

Methodology

The research design used to carry out this work is the narrative synthesis approach. This approach falls within the qualitative paradigm. It is a systematic review of existing studies in order to add an idea or shed more light on an issue of significance as well as contribute to the existing body of knowledge. Hence, the approach is based on the use of secondary sources, particularly journal articles, books, reports, and media reports. The synthesis of the current paper is structured thus:

development of the Internet, data privacy and protection, typologies of data privacy breaches and attacks, protection strategies, and the challenges of data privacy protection in the Nigerian digital space.

Conceptual Clarifications

Concept of Digital Abyss

The concept of "Digital Abyss" connotes the current scenario where societies are overwhelmingly dependent on the Internet and digital media such as the Internet, smartphones, and laptops, among others. It also represents the challenge of information overload and management (Wardle & Derakhshan, 2017). Furthermore, it involves concerns regarding privacy and data security while using the Internet. As noted by Brynjolfsson and McAfee (2014), the increasing dependence on the led to volume, velocity, and variety of data generated through various sources such as social media, IoT devices, and online transactions. With digital media, personal data can be used to track Internet users as well as put the user under surveillance by different actors without the users' knowledge. There are intrusive innovations that record our voices and even our secrets under our roof without our knowledge. For example, powerful digital media like Google and Apple regularly hear confidential medical information, business deals, and recordings of couples having sex without their people's knowledge (Hern, 2019). The modern generation is indeed in an abyss that is impracticable to come out. However, ethical frameworks, robust cyber-security measures, digital literacy programmes, and regulatory interventions mitigate the risks (Floridi, 2019).

Internet Privacy

The concept of privacy has been studied from antiquity to the modern world, from philosophical, sociological, psychological, and legal perspectives. In modern times, several academics in various fields have attempted to define privacy, yet there is no universally agreed definition of the term in academic research. This led to the conclusion that the concept is an umbrella term that covers a wide range of interests. According to Veghes, Pantea, Balan, and Lalu (2009), privacy covers all issues relating to the protection of an individual's personal space, i.e., private life, private home, private correspondence, and so on. Explicitly, Burgoon (1982) observed that the dimensions of privacy include information or data privacy, physical privacy, social privacy, and psychological privacy. The current study is concerned with information privacy, also referred to as data piracy.

Alan F. Westin, who is considered the pioneer of the modern concept of privacy, defines information privacy as the claim of an individual or a group or organisation to determine when, how, and to what extent information about them can be communicated to others (Rollenhagen, 2021). Nyoni, Velempini, and Mavetera (2020) observe that the emergence of the Internet and other new technologies has furthered the scope and definitions of what constitutes data privacy. Smith goes on to describe data privacy as holding control over what information about the user could be circulated. Taylor, Davis, and Jillapalli (2009) further explain that privacy in the online environment covers users' concerns about the type and quality of information that a particular website will collect from the user during online activity, how much control users have over the collected information, and users' awareness of the privacy practices of websites, sites, and digital devices.

Personal Data Safety

Personal data safety refers to the protection, security, and responsible handling of individuals' sensitive and identifiable information. It involves safeguarding personal data from unauthorised

access, misuse, theft, or any form of exploitation that could lead to potential harm or compromise individuals' privacy (Shea, 2022). Li and Liu (2021) also explain that personal data safety has a relationship with the protection of software and hardware. This is because it is attacks on the software through malware, hacking, etc. that give access to users' personal information. Personal data safety is necessary for effective Internet and new media engagement. Many people are hesitant to use the Internet and new media due to fear of their personal data safety.

One of the fundamental aspects of personal data safety in digital media is user awareness and education. Individuals must understand the risks associated with sharing personal information online and take proactive measures to safeguard their data. Aside from individuals, the government has the responsibility to establish policies geared towards ensuring cyber safety and implement them. Other stakeholders in data privacy protection on the Internet include website owners, app developers, and platforms such as social media (Perera, Ranjan, Wang, Khan, & Zomaya, 2015).

Discussion

Data Privacy Breaches and Attacks on the Internet

Data collection in the digital world is too sophisticated. Several ways have been identified by extant literature regarding how personal information is syphoned and used by different parties on the Internet. Abrams (2014) noted that personal data are revealed by choice, for example, through social media and email; in other situations, through compulsory disclosure, for example, as a pre-condition to receiving services; or without awareness or consent, for example, by tracking an individual's browsing. In the same vein, Rust, Kannan, and Peng (2002) assert that service providers collect the personal data of users while registering or opening an account, like social media accounts, online registrations and applications of all kinds, online surveys, and contests, among others. Rust *et al*. explained that when personal data is collected via the aforementioned strategies, the data collectors store it in their database and then sell or communicate it to other third parties for monetary gains such as target advertising, ultimately eroding the privacy of the individual customer.

The ever-increasing appetite for harvesting, analysing, and using the personal data of new media users has led service providers, app developers, and manufacturers of smart devices and big tech companies to establish increasingly pervasive and innovative ways of harnessing the data of users through innovations like sensors, which track not just what a user types on a given device but record the voice or discussion and even videos of the users without the user knowing, thus overstepping privacy boundaries (Birchley, Huxtable, Murtagh, ter Meulen, Flach & Gooberman-Hill, 2017).

Other privacy-intrusive methods of data collection employed by Internet companies or sites are cookies and Clickstream (Brian, 2003). A cookie enables a website server to develop a history of communication between a user and the website visited. With the help of a cookie, a server can keep track of sites a user visits and the kind of information searched. Clickstream is a more sophisticated way of data collection; it collects data about sites visited by a user, the kind of information searched, and the duration of time spent on each site. Both cookies and clickstream collect the personal data of users and send the same to databases on the control systems of companies that later use it for various purposes.

It is also important to note that the personal information of consumers could also be accessed from the hosting site or company without the site's or company's collaboration. This phenomenon is

popularly called hacking. Grimes (2017) described hacking as the act of exploiting the weaknesses in a computer of another individual or gaining access to a network without permission to steal, destroy, or change the information on the computer. Once a computer, website, or account is hacked, the hacker gains access to the user's information, including privacy or confidential information that can be used for malicious purposes. The weaknesses that give room to hacking include traceable passwords and exposure to malicious software, particularly viruses or Trojan horses. Others are exposed to users' cookies, otherwise known as session keys, to gain unauthorised access to information or services on a computer system. This is usually directed at e-commerce websites where users provide personal information for a transaction (Khanna & Chaudhry, 2012). Another strategy hackers use to steal the personal data of users online and use it for malicious purposes is known as phishing. Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by setting up a replica of an original site (Ramzan, 2010). The phisher deceives people by using similar e-mails to those mailed by well-known enterprises, for example, banks. These e-mails often ask users to provide personal information or result in users losing their rights; they usually contain a counterfeit URL that links to a website where the users can fill in the required information. Phishers base their strategy on using psychological or emotional triggers, such as inducing fear in the users or generating some sort of curiosity in the users. More often, phishers use statements such as "your account has been compromised" or "your account will be disabled, and then request that you perform a given task, such as clicking a link (Khanna & Chaudhry, 2012). Chen, Jeng and Liu (2006) also argued that people are often trapped by phishing due to inattention.

Data Privacy and Protection Strategies on the Internet

Extant literature categorizes data privacy protection strategies on the Internet into three categories: the use of privacy-enhancing technologies, self-protection strategies, and legal or legislative measures. Privacy-enhancing technologies (PETs) are software designed by Internet service providers to increase the privacy and security of sensitive data such as names, phone numbers, email addresses, and social security numbers of users (Office of the Privacy Commission Canada, 2017). PETs allow users to protect their information or privacy by allowing the user to decide what information he or she is willing to share with third parties, such as online service providers, under what circumstances that information will be shared, and what the third parties can use that information for (Fang & Lefevre, 2010). There are many different types of PETs, each designed to solve a specific problem. One common example of PETs is the privacy setting feature available on smartphones and websites, such as social networking sites. The most important thing about the use of privacy settings is for the user to understand the feature and carefully choose settings that minimize the user's vulnerability to malicious users and third parties. One major issue associated with privacy settings is that the privacy settings of many websites, especially social networking sites, are often complex.

The second line of protection against digital data breaches and cyberattacks lies with the individual Internet user; hence, it is called self-protection behavior. Protective behaviours are defined as "specific computer-based actions that consumers take to keep their information safe" (Milne, Labrecque, & Cromer, 2009, p. 450). One of these measures is to understand the privacy settings of websites, study policies, or the terms and conditions of service providers regarding the use of consumers' data, make an informed decision whether to use a given Internet service or not, and carefully configure privacy settings to protect online data leakage (Williams, Consalvo, Caplan, & Yee, 2009). Other personal protective strategies identified by Williams *et al* are the need to limit

the posting of personal information details on the Internet, especially social media, and being careful when dealing with strangers online. Also, Rajasekharaiah, Dule and Sudarshan (2020) suggested the use of unique and strong passwords as a means to enhance data security on the Internet and new media. A good password, according to Tabassum (2020), entails a combination of letters, numbers, and special characters and is frequently changed. In addition to the above, PricewaterhouseCoopers [PwC] (n.d.) states that individuals can enhance their cyber security or safety by incorporating multi-factor authentication wherever possible and that having more than one form of authentication, such as using a password and a soft or hard token on personal devices and accounts, provides a strong line of defense against personal data exploitation by attackers.

In another dimension, Maimo (2019) asserts that anti-virus protection has been the most prevalent solution to fight unsuspecting cyber-attacks. Active anti-virus blocks viruses designed and developed by cybercriminals from entering the user's device to compromise, corrupt, manipulate, or steal personal data. In another development, Mediati (2011) asserts that while using public computers, care must be taken because public computers can easily be infected with spyware and other types of malwares devised to track movements online and collect passwords. Similarly, Diallo (2014) asserts that cyber attackers sometimes set up rogue Wi-Fi networks disguised as legitimate ones to steal personal information. Therefore, Internet users should always verify the public network before connection, and that public network should not be used to check e-mails, use social network accounts, conduct online banking, or perform any other action that entails logging in to a site (Diallo, 2014). Similarly, Chen, Jeng an Liu, (2006). further explain that individual users can enhance their privacy protection by deleting cookies or browsing history at the exit of browsers, especially when using public or another person's Wi-Fi networks or devices: The users should always clear the cookies manually or set up the configuration on browsers to automatically delete them as soon as the browser session ends. Kaspersky Lab (2022) further states that keeping a device's operating system up-to-date allows for benefiting from the latest security patches that help the cyber user avoid falling prey to cybercriminals. Furthermore, PwC states that Internet users can enhance their safety if they avoid opening or clicking on emails and attachments from unrecognized sources.

The third protection strategy is the legal or legislative strategy. Over 128 countries in the world have set in place data protection and privacy legislation to ensure that their citizens' data is safe (UNCTAD, 2020). In Nigeria, there are different sectoral legislations geared towards protecting Internet consumers. Examples are the Cybercrimes Prohibition, Prevention, etc. Act, the Registration of Telephone Subscribers Regulations, and the Credit Reporting Act, among others. However, the National Data Protection Regulations (NDPR) are so far the most comprehensive instrument designed to explicitly address the problem of digital data privacy breaches in Nigeria (Babalola, 2022). NDPR is the brainchild of the National Information Technology Development Agency (NITDA). NITDA was initially commissioned as an office with the main objective of providing information and communication technology tools to selected educational institutions in Nigeria (Babalola, 2022). It, however, became a statutory body upon the enactment of the NITDA Act, 2007, thus giving the agency express powers to, among other functions, coordinate and monitor information technology practices, develop guidelines for election governance (e-governance), and monitor the use of electronic data interchange (EDI) (NITDA, 2020).

Challenges of Digital Data and Privacy Protection in Nigeria

As Internet penetration continues to grow in Nigeria amidst a burgeoning population, data privacy protection is becoming more complex and challenged by different factors. The first challenge is poor enlightenment campaigns. The issue of digital data privacy protection education has yet to receive significant attention from stakeholders like mass media, civil society, data collectors, and government agencies such as national orientation agencies and the Ministry of Information. So far, there are no significant social mobilisation campaigns and enlightenment programmes in both mass media and other channels of communication geared towards equipping Nigerians with knowledge about data privacy rights and protection mechanisms. Even the ambitious NDPR has not received the significant publicity it deserves; hence, many Nigerians do not know about the existence of the regulations or how they are meant to protect them (Alao, 2022).

Secondly, there is the phenomenon of high illiteracy. Nigeria is one of the countries with a high rate of illiterate citizens. This is more so as it relates to digital illiteracy and, in particular, data protection (Akanbi & Akanbi, 2012). Alao (2022) asserts that Nigerians are generally unaware of their rights, including the right to digital data and privacy protection. Therefore, there has been a culture of silence or underreporting of data breaches and attacks. Similarly, the National Information Technology Development Agency (2020) states that more and more people are adopting the Internet in Nigeria, but the vast majority of the Nigerian population that uses the Internet is unaware of the dangers associated with it or how to use self-protection mechanisms to mitigate data breaches and attacks. It has also been observed that many Nigerians depend on third parties to help them access Internet services such as online purchases and online registrations of all kinds or use certain digital devices like smartphones.

Thirdly, there are the economic realities and priorities facing Nigerians. Poverty is high, and there is a dearth of basic infrastructure such as good roads, hospitals, water, electricity, and schools, among others (World Bank Group, 2022). These challenges have taken the attention of both government and citizens and have always been on the agenda of discussion in the media and other platforms. Thus, the government is reluctant to pass substantive laws to protect the personal data of citizens in the digital space as well as adequately fund data protection agencies and security to actualize the primary assignment. Similarly, the citizens are interested in pursuing their "daily bread," hence they are also reluctant to pursue their rights even when such rights are breached or when they experience cyber-attacks, seeing such acts as a waste of time and resources.

Another problem facing digital data privacy protection in Nigeria is systemic corruption. Corruption has created a culture of lack of trust in Nigerian agencies, institutions, and programmes, no matter the sincerity behind their establishment. Today, many Nigerians do not trust the ability and sincerity of Nigerian security agencies to protect against cyber-attacks and personal data breaches prevalent in the nation's digital space. Therefore, Nigerians are often unwilling to support the agencies with useful information towards enhancing cyber sanity in the country. This challenge is compounded by the general poor implementation of laws and recommendations that will improve the nation’s development in different sectors, including cyber security.

Conclusion and Path Forward

The Internet is both a blessing and a threat to our safety, as issues of data privacy breaches and attacks can have significant implications for the safety of users in real life. Therefore, as we leverage the Internet to build businesses, access information and health, and build relationships,

among other gratifications, care must be taken by the users to navigate the digital abyss without falling prey to bad actors and malicious users who have committed digital data theft and breached their major occupations. To actualize that, the users need adequate sensitization campaigns that are tailored to provide both knowledge of the risks and protection strategies of cyber-attacks and data breaches. This can only be achieved by a combined effort of multiple stakeholders, ranging from the mass media, education curriculum planners at all levels, government agencies like NITDA, the Ministry of Information, and national orientation agencies, among others. Until these stakeholders rise up and become intentional about ensuring a safer cyberspace, the ambitious digital economy will remain a mirage.

References

Abrams, M. (2014). *The Origins of Personal Data and its Implications for Governance*, http://dx.doi.org/10.2139/ssrn.2510927.

Akanbi, B., & Akanbi, C. (2012). Bridging the Digital Divide and the impact on poverty in Nigeria. *Advances in Multidisciplinary &Amp; Scientific Research Journal Publication*, 3(4), 81–87. https://doi.org/10.22624/aims/cisdi/v3n4p2x

Alao, O. (2022, March 30). *The Nigeria Data Protection Bureau and the challenges of Data Privacy Compliance in Nigeria*. https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-data-protection-bureau-and-the-challenges-of-data-privacy--compliance-in-nigeria

Alkhalil, Z., Hewage, C., Nawaf, L. & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Front. Computer. Science,* 3:563060. doi: 10.3389/fcomp.2021.563060

Babalola, O. (2020). *Data Protection and Privacy Challenges in Nigeria (Legal Issues)*. https://www.mondaq.com/nigeria/dataprotection/901494/data-protection-and-privacy-challenges-innigeria-legal-issues

Birchley, G., Huxtable, R., Murtagh, M., ter Meulen, R., Flach, P., & Gooberman-Hill, R. (2017). Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC Medical Ethics*, 18(1). https://doi.org/10.1186/s12910-017-0183-z

Brian. K.G. (2004). Personal privacy on the Internet: Should it be a Cyberspace entitlement? *Indiana Law Review*, 36:827

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company.

Chen, W. & Wellman, B. (2005). Charting digital divides: Comparing socioeconomic, gender, life stage, and rural-urban Internet access and use in five countries. *Transforming Enterprise*. 467-497.

Chen, T., Jeng, F. & Liu, Y. (2006). Hacking tricks toward security on network environments. *IEEE*, pp. 442.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism (Culture and economic life)*. Stanford, CA: Stanford University Press.

Diallo, A. (2014). *How to avoid data theft when using public Wi-Fi*. Retrieved from: http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers- love-public-wi-fi-but-youcan-make-it-safe/

Daily Amar Desh, (19th June 2014). Bangladesh. Available at:

https://mybangla24.com/newspapers/amardesh

Eddy, M. (2018, October 10). *How companies turn your data into money*. PCMAG. https://www.pcmag.com/news/how-companies-turn-your-data-into-money

Fang, L. & LeFevre, K. (2010). Privacy wizards for Social Networking Sites. Conference: *Proceedings of the 19th International Conference on World Wide Web*, Raleigh, North Carolina, USA, April 26-30, DOI:10.1145/1772690.1772727

Floridi, L. (2019). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophy & Technology*, 32(1), 1-8.

Freeze, D. (2019, July 27). Humans on the Internet will triple from 2015 to 2022 and hit 6 Billion. Retrieved from: *Cybercrime Magazine*. https://cybersecurityventures.com/how-many-Internet-users-will-the-world-have-in-2022-and-in-2030/

Goldstein, K., Tov, O.S & Prazeres, D. (2018). The Right to Privacy in the Digital Age. A Paper presented on behalf of *Pirate Parties International Headquarters*, a UN ECOSOC Consultative Member, for the Report of the High Commissioner for Human Rights. Retrieved from: https://www.ohchr.org/sites/default/files/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf

Grimes, R.A. (2017). *Hacking the hacker: Learn from the experts who take down hackers*. John Wiley & Sons.

Hern, A. (2019). Apple contractors "regularly hear confidential details" on Siri recordings. *The Guardian*. https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings

Identity Theft Resource Center. (2020). *ITRC 2019 end of year data breach report.* Retrieved from https://www.idtheftcenter.org/2019-data

Jaffe, J. (2002, December 31). Happy Birthday, Dear Internet. *WIRED*. Retrieved from https://www.wired.com/2002/12/happy-birthday-dear-Internet/

Kaspersky Lab. (2022, February 17). Ransomware protection: How to keep your data safe in 2022. *www.kaspersky.com*. https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

Kemp, S. (2022, February 1). *Digital in 2019: Global Internet Use Accelerates. We Are Social* UK. https://wearesocial.com/uk/blog/2019/01/digital-in-2019-global-Internet-use-accelerates/

Khanna, S. & Chaudhry, H. (2012). "Anatomy of compromising email accounts," *2012 IEEE International Conference on Information and Automation*, Shenyang, China, 2012, pp. 640-645, doi: 10.1109/ICInfA.2012.6246756.

Li, Y. & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Rep. 7, 8176–8186. doi: 10.1016/j.egyr.2021.08.126

Maimon, D. (2019). *Existing Evidence for the effectiveness of antivirus in preventing Cyber Crime Incidents. EBCS Tools*. 6. Retrieved at: https://scholarworks.gsu.edu/ebcs_tools/6

Marr, B. (2018). *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*. Forbes. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=2626c67660ba

Marquardt, F. & Breinstrup, T. (2019) Skruen strammes om Apple og Google efter nye danske

aflytningssager Berlingske https://www.berlingske.dk/virksomheder/skruen-strammes-om-apple-og-google-efternye-danske-aflytningssager - last accessed on 12-05-2020

McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. *Harvard Business Review* 90:60– 68.

Mediati, N. (2011). *Secure Your Life in 12 Steps*. Retrieved at:http://www.pcworld.com/article/225806/secure_your_life_in_12_steps.html

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, 43(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

NITDA (2020). Nigeria Data Protection Regulation 2019: Implementation Framework. Retrieved at: https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

Nyoni, P.; Velempini, M. & Mavetera, N. (2020). Emerging Internet Technologies and the Regulation of User Privacy. The African Journal of Information Systems: 13. (1) , Retrieved at: https://digitalcommons.kennesaw.edu/ajis/vol13/iss1/1

Odufuwa, F. (2021). Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries [*Nigeria Report* 179-211]. Published by the African Declaration on Internet Rights and Freedoms Coalition, Available at: https://africanInternetrights.org

Office of the Privacy Commissioner of Canada. (2017). *Privacy Enhancing Technologies – A Review of Tools and Techniques*. Retrieved at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/

Ololuo, F. (2020). *Nigeria: "Whoever controls your data controls your life": Why your data should be protected*? Retrieved from: http//www.mondaq.com/nigeria/data-protection/933184/whoever-controls-your-data-controls-your-life-why-your-data-should-be-protected-francis-ololuo

Perera, C. Ranjan, R., Wang, L. Khan, S. U. & Zomaya, A. Y. (2015). "Big Data Privacy in the Internet of Things Era," in *IT Professional*, vol. 17, no. 3, pp. 32-39, May-June 2015, doi: 10.1109/MITP.2015.34.

Shea, S. (2022b). *What is data se curity? The ultimate guide*. Security. https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know

Pew Research Center (2022). *Stories from experts about the impact of digital life*. Internet, Science & Tech. https://www.pewresearch.org/internet/2018/07/03/the-positives-of-digital-life/

PricewaterhouseCoopers. (n.d.). *Cybersecurity and Privacy in Nigeria*. PwC. https://www.pwc.com/ng/en/publications/cybersecurity-and-privacy-in-nigeria.html

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering*, 981(2), 022062. https://doi.org/10.1088/1757-899x/981/2/022062

Ramzan, Z. (2010). *Phishing Attacks and Countermeasures. Handbook of Information and Communication Security*, 433–448. Retrieved at: https://doi.org/10.1007/978-3-642-04117-4_23

Rollenhagen, L. (2021, January 15). *Alan Westin is the father of modern data privacy law. Osano*. Retrieved at: https://www.osano.com/articles/alan-westin

Rust, R., Kannan, P. K. & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of The Academy of Marketing Science*, 30. 455-464. 10.1177/009207002236917.

Schumacher, S., & Kent, N. (2020, July 27). *8 charts on Internet use around the world as countries grapple with COVID-19.* Pew Research Center. Retrieved at: https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-Internet-use-around-the-world-as-countries-grapple-with-covid-19/

Sobolewski, M., Mazur, J. & Paliski, M. (2017). GDPR: A step towards a user-centric Internet? *Intereconomics, 52*(4), 207-213. http://dx.doi.org/10.1007/s10272-017-0676-5

Statista. (2023, February 9). Web traffic by device in Nigeria 2023. https://www.statista.com/statistics/1323401/web-traffic-by-device-in-nigeria/#:~:text=As%20of%20January%202023%2C%20most,a%20share%20of%200.71%20percent

Tabassum, L. (2020). Cybersecurity and Safety Measures. *International Research Journal of Modernization in Engineering Technology and Science*, 2 (6).

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3), 203–223. https://doi.org/10.1007/s10660-009-9036-2.

UNCTAD (2016, April 19). *Data protection frameworks must be compatible with international data flows for developing countries to benefit from the global digital economy*. Retrieved from:https://unctad.org/news/data-protection-frameworks-must-be-compatible-international-data-flows-developing-countries

Veghes, C., Pantea, C., Balan, D. &Lalu, B. (2009). European Union consumers 'views on the protection of their personal data: an exploratory assessment. Annales Universitatis Apulensis: Series Oeconomica, 11(2). Retrieved from: https://EconPapers.repec.org/RePEc:alu:journl:v:2:y:2009:i:11:p:44.

Vicente, M. & Lopez-Menendez, A. (2008). Some empirical evidence on Internet diffusion in the New Member States and Candidate Countries of the European Union. *Applied Economics Letters, Taylor & Francis Journals*, 15(13), 1015-1018. DOI: 10.1080/13504850600972352

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe report.

Williams, D., Consalvo, M., Caplan, S., & Yee, N. (2009). Looking for Gender: Gender Roles and Behaviors Among Online Gamers. *Journal of Communication*, 59(4), 700–725. https://doi.org/10.1111/j.1460-2466.2009.01453.x

World Bank Group. (2022, March 22). *Deep Structural Reforms Guided by Evidence Are Urgently Needed to Lift Millions of Nigerians out of Poverty, says New World Bank Report. World Bank.* https://www.worldbank.org/en/news/press-release/2022/03/21/afw-deep-structural-reforms-guided-by-evidence-are-urgently-needed-to-lift-millions-of-nigerians-out-of-poverty.