Galactica Media: Journal of Media Studies. 2024. No 3 | ISSN: 2658-7734
Новые медиа и коммуникации | https://doi.org/10.46539/gmd.v6i3.489

Privacy Awareness and Social Media: Personal Data Protection among Facebook** and Instagram** Users

Dede Ibiere Peter[1] & Ben-Collin Emeka Ndinojuo[2]

University of Port Harcourt. Port-Harcourt, Nigeria

Received: 29 February 2024 | Revised: 18 May 2024 | Accepted: 30 May 2024

Abstract

This study investigated the level of awareness of personal data protection among Facebook** and Instagram** users. The research evaluated the number of Facebook and Instagram users who have taken precautions to secure their personal data, why they did so, and the identification of regulatory authorities responsible for data protection in Nigeria. The Privacy Calculus Theory was used as the theoretical framework. The survey research design was used for this study, with the web-based questionnaire as the instrument for data collection. A sample size of 396 was drawn from the student population at the University of Port Harcourt. The data were analyzed in tables using frequency and percentage. The results indicated that users are strongly aware of the significance of safeguarding personal data on Facebook and Instagram. The users acknowledged implementing precautionary steps to safeguard their personal data. However, they still need to determine the specific agencies and regulatory entities accountable for ensuring the safety of personal data. In order to tackle this problem, the study recommended that the University management and student bodies should organize specific educational workshops to promote understanding of the pertinence of safeguarding personal data on social media platforms (Solove, 2021), create easily accessible materials and guidelines on the University of Port Harcourt portal designed for social media users, outlining the best methods for protecting personal data, including personal data protection awareness in its orientation programs and student events and also set up a system for reporting potential data breaches and offer assistance to affected users.

** – A social network owned by "Meta", which is recognized as extremist in Russia

Keywords

Privacy Awareness; Social Media; Facebook; Instagram; Data Security; Privacy Settings; Privacy Education

This work is licensed under a Creative Commons "Attribution" 4.0 International License

1 Email: pdede[at]mmcasafo.com
2 Email: ben.ndinojuo[at]uniport.edu.ng ORCID https://orcid.org/0000-0003-4163-7756

Galactica Media: Journal of Media Studies. 2024. No 3 | ISSN: 2658-7734
New Media and Human Communication | https://doi.org/10.46539/gmd.v6i3.489

Осведомленность о конфиденциальности и социальные сети: защита персональных данных среди пользователей Facebook** и Instagram**

Питер Деде Ибиер[1], Ндиноджуо Бен-Коллин Эмека[2]

Университет Порт-Харкорта. Порт-Харкорт, Нигерия

Рукопись получена: 29 февраля 2024 | Пересмотрена: 18 мая 2024 | Принята: 30 мая 2024

Аннотация

В этом исследовании изучался уровень осведомленности относительно защиты персональных данных среди пользователей Facebook** и Instagram**. Исследование оценивало количество пользователей Facebook и Instagram, которые приняли меры предосторожности для защиты своих персональных данных, причины принятия этих мер, а также регулирующие органы, ответственные за защиту данных в Нигерии. В качестве теоретической основы была принята теория Privacy Calculus Theory. В работе был использован дизайн опросного исследования с веб-анкетой в качестве инструмента для сбора данных. Выборка в 396 человек была взята из студенческого контингента Университета Порт-Харкорта. Данные были проанализированы и отражены в таблицах с указанием частоты и процента. Результаты показали, что пользователи хорошо осведомлены о важности защиты персональных данных на Facebook и Instagram. Однако им еще предстоит определиться с конкретными агентствами и регулирующими организациями, ответственными за обеспечение безопасности персональных данных. Для решения этой проблемы в статье рекомендуется, чтобы руководство университета и студенческие организации организовали специальные образовательные семинары для повышения понимания важности защиты персональных данных на платформах социальных сетей (Solove, 2021), создали легкодоступные материалы и руководства на портале Университета Порт-Харкорта, предназначенные для пользователей социальных сетей, в которых излагались бы лучшие методы защиты персональных данных, включая повышение осведомленности о защите персональных данных в программах ориентации и студенческих мероприятиях, а также создали бы систему сообщения о потенциальных утечках данных и предлагали помощь пострадавшим пользователям.

** – Социальная сеть, принадлежащая компании “Meta”, которая признана экстремистской на территории Российской Федерации

Ключевые слова

осведомленность о конфиденциальности; социальные сети; Facebook; Instagram; безопасность данных; настройки конфиденциальности; просвещение в области конфиденциальности

Это произведение доступно по лицензии Creative Commons “Attribution” («Атрибуция») 4.0 Всемирная

1 Email: pdede[at]mmcasafo.com
2 Email: ben.ndinojuo[at]uniport.edu.ng ORCID https://orcid.org/0000-0003-4163-7756

Introduction

The invasion of personal data on social networking sites has skyrocketed due to the undying quest by ICT companies to possess users' data (Barrett-Maitland & Lynch, 2020; Venugeetha et al., 2022). In the tech world, data is the key to every lock; it is a core determinant of what happens in the future of technology. It is an asset determining which ICT companies stay or get eliminated in the game. Data is the enabler for everything; you might call it the new currency, you might call it the new gold, you might call it the new oil. It is a fundamental part of the future, a basic part of the auto industry, and all the industries that are surrounding and integrating with it (Bhageshpur, 2019; Eludu et al., 2016; Shubladze, 2023). Data protection is highly regarded in Nigeria; Lambo et al. (2023) reviewed the principal data protection legislation and the relevant data protection sections in the Nigerian Constitution:

> The principal data protection legislation in Nigeria is the Nigeria Data Protection Act 2023 ("NDPA") which was signed into law by President Bola Ahmed Tinubu on 14 June 2023. The following laws and regulations impact data protection in Nigeria: The Constitution of the Federal Republic of Nigeria 1999 (as amended). The Nigeria Data Protection Regulation 2019 ("NDPR"). The NDPR Implementation Framework 2020, issued by the National Information Technology Development Agency ("NDPR Implementation Framework"). The Child Rights Act 2003. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. The Freedom of Information Act, 2011. The National Health Act, 2014. The HIV and AIDS (Anti-Discrimination) Act, 2014. The following sector-specific laws, regulations and guidelines have an impact on data protection in Nigeria: The Consumer Code of Practice Regulations 2007 ("NCC Regulations, 2007") published by the Nigerian Communications Commission ("NCC"). The Registration of Telephone Subscribers Regulations 2011, published by the NCC. The Consumer Protection Regulations 2020, issued by the Central Bank of Nigeria ("CBN"), Nigeria's apex bank. The Lawful Interception of Communications Regulations, 2019 which was issued by the NCC. The Guidelines for the Management of Personal Data by Public Institutions in Nigeria 2020, issued by the NITDA. The Official Secrets Act 1962. The CBN Guidelines on Point of Sale Card Acceptance Services 2011. The CBN Regulatory Framework for Bank Verification Number Operations and Watch-List for The Nigerian Banking Industry 2017. The NITDA Guidelines for Nigerian Content Development in Information and Communication Technology 2019 (as amended). The Credit Reporting Act 2017 (para. 1 – 2).

Social media has sparked extensive discussions about protecting user privacy because these platforms store personal information online. On Facebook[1], user-generated content plays a significant role as individuals freely express their thoughts, share personal photos, disclose their whereabouts, and provide details about their age and gender (Ihejirika et al., 2015; Keskin et al., 2023; Nwagwu & Akintoye, 2023). Unfortunately, many users are unaware of the potential risks of sharing personal data. They often trust Facebook as a secure platform, but this is only sometimes the reality (Barth et al., 2019; Das, 2022). One alarming concern is

1 Here and hereafter: A social network owned by "Meta", which is recognized as extremist in Russia

the possibility of hackers creating fake accounts or duplicating existing user accounts to gain access to personal information (Nyoni & Velempini, 2018). According to Kemp (2023), in January 2023, "the online presence of Nigerians on the two meta-platforms Facebook and Instagram[2] massively increased to 28.85 million, Facebook having 21.75 million and Instagram 7.10 million respectively".

As much as these Ads follow us everywhere, they do not. It is the website that hosts HTTP Cookies to track Users' browser history in order to target users. The Ads jumble up on our screens between scrolls on web pages we visit. As much as it has revolutionized how we communicate and share information, social media has also introduced numerous risks to our privacy and personal safety (Barrett-Maitland & Lynch, 2020; Ndinojuo & Ihejirika, 2015). In 2018, there were reports of data breaches affecting well-known brands like Facebook, Panera Bread, and Sacramento Bee, putting millions of personal records at risk of being misused by criminals. This suggests a profitable market for data, and hackers often sell stolen data to professional scammers. These statistics and incidents have led to widespread concerns about improving security systems for the personal data we provide. It is important to note that data protection laws cannot fully guarantee complete protection against malicious attacks, so users are encouraged to understand the basics of data privacy and take personal responsibility for their data security. Google, Uber, and Facebook have all experienced breaches that exposed users' private data over the years. In each case, these trusted companies failed to disclose the breaches promptly, preventing customers from taking necessary steps to protect themselves. Failing to report these violations emphasizes the importance of users taking personal data security seriously (Hill & Swinhoe, 2022; Obi, 2020; Siegel, 2018). This research aims to address Users' awareness of the risks associated with personal data on Facebook and Instagram, as well as provide solutions to foster the safeguarding of personal data to control cyber-attacks. It aims to assess the level of awareness among users regarding how their personal data is collected, stored, and used on these platforms and to identify key areas where improvements or educational efforts may be needed. The study examines how users are aware of personal data protection on Facebook and Instagram. The specific objectives include:

1. To evaluate the level of awareness of personal data protection among Facebook and Instagram Users.
2. To know how many users have taken precautionary measures to protect their personal data on Facebook and Instagram.
3. To find out the reason for the precautionary measures taken by Users to protect personal data.

2 Here and hereafter: A social network owned by "Meta", which is recognized as extremist in Russia

4. To identify the agencies and regulatory bodies responsible for personal data protection.

Based on the research objectives, the following research questions were proposed:

1. What is the personal data protection awareness level among Facebook and Instagram Users?
2. How many users have taken precautionary measures to protect their personal data on Facebook and Instagram?
3. What are the reasons for the precautionary measures taken by users to protect personal data?
4. What are the agencies and regulatory bodies responsible for personal data protection?

Privacy Calculus Theory

The Privacy Calculus Theory, formerly Behavior Calculus, was propounded by Laufer and Wolfe (1977). It postulates that individuals assess perceived privacy hazards and advantages before divulging personal data. They associated the concept of privacy with how individuals view specific events in their daily lives. Where the individuals perceive utility, they are willing to give up some of their privacy, while in contrast, if an individual perceives a greater level of danger associated with disclosing information in this specific context compared to other scenarios, they will be less inclined to provide information due to excessive concern about privacy issues. Based on the concept of privacy calculus, individuals using the Internet logically assess the disadvantages of privacy and the advantages of disclosing personal information (Fu et al., 2023; Princi & Krämer, 2020). The fundamental concept of the privacy calculus posits that when individuals perceive substantial advantages in a given circumstance, they are more inclined to engage in self-disclosure due to the outweighing of benefits over risks (Butori & Lancelot Miltgen, 2023; Tang & Ning, 2023).

In their study, a preregistered online experiment by Meir and Krämer (2022), participants (N = 485) were instructed to envision three disclosure scenarios where a privacy score indicated privacy risks. The study evaluated rational and intuitive decision-making approaches, as well as privacy resignation, as personality characteristics. The findings from a within-between random effects model indicated a positive relationship between benefit perceptions and self-disclosure intentions at both the between-person and within-person levels. The efficacy of the privacy score in facilitating users to make more privacy-conscious decisions at an individual level was determined. Ultimately, the rational decision-making style positively correlates with the sense of privacy risk. On the other hand, those who possess

a particularly intuitive decision-making approach can derive advantages from decision-making tools such as the privacy score.

Personal data protection

The General Data Protection Regulation (GDPR) places personal data at its core. It defines personal data as any information that pertains to a known or identifiable individual, also referred to as a data subject. Personal data is information specifically about a person (Finck & Pallas, 2020; Gazi, 2020). The GDPR further specifies that personal data includes any information that can identify a person directly or indirectly, such as their name, identification number, location data, online identifier, or factors unique to their physical, physiological, genetic, mental, economic, cultural, or social identity. Depending on the context, this covers a wide range of information, including someone's IP address, hair colour, occupation, or political opinions (Irwin, 2022; Lynskey, 2023). McDonald (2023) further explains that data protection refers to laws regulating access to personal information. Data protection typically grants individuals the right to access and request the rectification of data about themselves. Data protection governs the processing of data by organizations and restricts third-party access to personal data.

According to Crocetti et al. (2021), personal data can include various things such as names, photos, email addresses, bank account details, social media posts, biometric data, and even the IP address of a person's computer. Data protection is the process of safeguarding this valuable information from being corrupted, compromised, or lost. With the rapid growth of data being created and stored, the importance of data protection continues to elevate (McDermott, 2023; Paul et al., 2023). Minimizing any downtime that could prevent access to important information is crucial. Therefore, a significant aspect of a data protection strategy is ensuring that data can be quickly restored in case of corruption or loss. Aside from that, protecting data from compromise and ensuring data privacy are also essential elements of an effective data protection approach (Acquisti et al., 2016; Marelli, 2023; Obi, 2020).

In a study conducted by Ee (2023), it was shown that a significant proportion of social media users in Malaysia are inclined to reveal personal details about their family and finances. This is because they perceive social media as a secure platform, as long as they restrict access to their social media profiles to just those individuals whom they know and trust. A similar outcome arose from the study of Das (2022) regarding the awareness of data privacy while using social networks in Bangladesh. The research conducted by Külcü and Henkoğlu (2014) demonstrates that information professionals in Turkey are concerned about privacy, and a majority of users actively modify the default settings to safeguard their private data. This was reinforced by Gogus and Saygin (2019) that high school students in Turkey were very concerned about their privacy online. The Pew Research Centre found that 80% of social media users expressed appre-

hension over advertising and corporations accessing their personal information on social media platforms. Additionally, a significant majority of 74% of users place great importance on having control over the individuals who can gain privy to their private data (Rainie, 2018). Madden (2012) stated that privacy is a primary concern for users of social media platforms, while Benisch et al. (2011) aver that social media users perceive a lack of control over their privacy as one of their biggest worries.

The concept of Awareness

Awareness refers to having knowledge, being conscious, staying informed and alert. It represents the state or capability to perceive, feel, or be conscious of events, objects, or sensory patterns (Pala, 2023; Sattin et al., 2021). In this state of consciousness, an observer can confirm the presence of sensory information without necessarily having a deep understanding of it. While possessing knowledge requires having awareness, it is important to note that mere awareness does not necessarily equate to knowing any kind (Majolo et al., 2023; Tisserand et al., 2023). Jati et al. (2019) specify that "Awareness is more about personalization, perceiving, and self-focus; therefore, it depends on and directs to personal concerns to respond to something" (p. 3). Bhasin (2022) explains that awareness is the cognitive state in which an individual consciously understands a specific circumstance or object. It can also be interpreted as the capacity to perceive or comprehend something.

Therefore, when organizations or brands endeavor to enhance awareness regarding their products or services, they strive to provide information and educate the intended audience about them (Coronado-Maldonado & Benítez-Márquez, 2023; Maddocks, 2023). *Awareness* is the cognitive state characterized by a thorough understanding of the subject or circumstance. For instance, self-awareness would involve becoming cognizant of various facets of your emotional intelligence, behavioural tendencies, emotions, personality characteristics, etc., through introspection and contemplation.

One's awareness can be enhanced by knowing one's surroundings. It aids in perceiving information about one's environment and facilitates the direction of related ideas (London et al., 2023; Pretorius & Plaatjies, 2023).

Overview of the Nigerian general data protection law

Since the invention and proliferation of the internet, it has significantly transformed how we share information and eliminate barriers. Nonetheless, as technology continues to progress and becomes more advanced, we must also acknowledge the potential hazards linked to digital privacy breaches, cybersecurity threats, and the responsible and ethical handling of data (Gielens & Steenkamp, 2019; Milligan, 2022; Warren, 2022). Oturu (2019) reveals that historically, organizations

employed several techniques such as anonymization, pseudonymization, encryption, key-coding, and data sharing to separate data from actual identities. Data protection and privacy are an amplification of the inherent entitlement of individuals to privacy (Westin, 2003), Section 37 of the 1999 Constitution (as modified) safeguards the rights of individuals to maintain the confidentiality of their personal information and the privacy of their residences, written communications, phone conversations, and telegraphic messages. In addition to the Constitution, various other legislations include rules pertaining to safeguarding data and privacy. One of these laws is the Freedom of Information Act No. 4 of 2011, which grants the public access to public records and information. It also prohibits public institutions from exposing personal information to the public without the approval of the individuals affected.

King'ori (2023) informs that the President of Nigeria signed the Data Protection Bill into law on June 12, 2023, after it passed the third reading in both the Senate and the House of Representatives. The Data Protection Act of 2023, often known as the Act, has received executive and legislative backing. It is a significant achievement in Nigeria's nearly twenty-year effort to establish comprehensive data protection legislation. In September 2022, the National Commissioner of the Nigeria Data Protection Bureau (NDPB), now known as the National Data Protection Commissioner (NDPC), declared that the office would pursue legal assistance to establish a new law as a component of the Nigeria Digital Identification for Development Project. The statute was, after that, subjected to a certification process in October 2022. After validation, the Act was submitted to the Federal Executive Council for approval, which prepared the path for its transmission to the National Assembly. The Nigeria Data Protection Bill, 2023, was introduced in both chambers of Nigeria's bicameral legislature as the 2022 Data Protection Bill. The Act took effect immediately after being signed by the President. The Act encompasses data protection concepts widely shared among several international data protection regimes. The term "personal data" is defined to cover legal responsibilities for both data controllers and processors, which are defined comparably to the majority of data protection laws globally.

Data protection challenges on Facebook and Instagram

It is undeniable that Facebook and Instagram are among the most popular platforms, generating the highest number of likes (Dixon, 2023; Lyons, 2023). However, despite their enormous user base, these applications have yet to assure users of their privacy. Facebook, in particular, has faced intense scrutiny in recent years due to its failure to create a secure environment where user accounts and profiles remain private. This has resulted in various actions taken by Facebook without user consent, jeopardizing the privacy of its users (Lauer, 2021; Quach et al., 2022). The current generation of users is greatly concerned about their online image and the impression they make on their profiles. Thus, some users must verify who

they are adding to send friend requests to as many people as possible. Also, in their attempts to expand their friend list, some users accept requests from strangers or receive friend requests from strangers due to technical glitches. These users easily access private information about others, including sensitive details like location. Regrettably, Facebook frequently updates its privacy policies without adequately considering user opinions (Lajnef, 2023; Marcelline, 2023). When a platform with as many users as Facebook plans to change its privacy policy, it should inform users in advance. Personal notifications should be sent to all users, allowing them to adjust their privacy settings accordingly to avoid any negative impact caused by the policy changes (Dennis, 2019; Nissenbaum, 2010; Schneier, 2015).

Ja'han (2023) informs that Ireland's authorities imposed a fine of over $400 million on Meta, the parent company of Facebook and Instagram, for breaching European Union regulations regarding acquiring and managing user data by technology companies. Furthermore, the social media giant may have other challenges in the future. The primary concern centers on Facebook and Instagram's dependence on users' data to inundate them with tailored advertisements. The very intrusive advertisements are a significant revenue stream for most social platforms. However, like other countries in the European Union, Ireland enforces stringent regulations around accessing and utilizing users' private information by social networking platforms and other technology businesses. Ireland's substantial penalties arise from two complaints against Meta in 2018, alleging that the business coerced customers into consenting to utilize their data for personalized advertisements.

Lomas (2021) discloses that recent research by Fairplay, Global Action Plan, and Reset Australia reveals that Facebook continues to monitor teenagers for targeted advertising on its social media platforms. This finding contradicts Facebook's earlier announcement during the summer, in which the technology giant asserted that it would restrict advertisers' ability to target children. Following a continuous series of controversies, Facebook recently changed the name of its group business to "Meta" in an apparent attempt to rehabilitate its reputation. Facebook/Meta is facing a new issue as it has been accused of not truly discontinuing ad targeting for teenagers. According to research, the company has kept its algorithms' capacity to monitor and focus on children, allowing its artificial intelligence systems to surveil young individuals. This enables Facebook/Meta to utilize online activity data to determine the most suitable advertisements to display, increase user interaction, and enhance its advertising revenues.

Vilic and Radenkovic (2015) clarified that on further scrutiny of Facebook, it becomes apparent that the primary inclination is to maximize the accessibility of users' data to the general public browsing the virtual realm of the Internet. This is because, upon user registration, all personal data are initially set to the lowest level of privacy protection, and it is only when the users establish specific restrictions that this changes. Users of this social network can customize their privacy settings, allowing them to safeguard their privacy to varying extents.

To register for a Facebook account, users must provide their name, email address, date of birth, and gender, as stated in Facebook's Privacy Policy. The data above, encompassing the profile image, username, and password, becomes accessible to the general public on the Internet. Whenever a user registers to access their personal Facebook page, views the profiles of others, searches for a specific page or friend, clicks on an advertisement on the page, or interacts with any application, Facebook acquires, gathers, and retains this data. Additionally, if a user uploads a picture or video, Facebook logs the precise time, date, and location of when the respective media appeared. Data is gathered and stored irrespective of the method or origin from which it was transmitted to the profile.

Curtberthson (2021) identified Instagram at the top of the list of "invasive apps" that collect and share users' data. pCloud, a cloud storage company, identified this finding by analyzing the newly implemented app privacy labels, now mandatory for firms to include in Apple's App Store. According to the report, Instagram acquires and shares 79 percent of its users' personal information with external entities, such as search history, location, contacts, and financial details. When you agree to share information with an app during the sign-up process, they can analyze it to their advantage and share it with others. In a blog post, Ivan Dimitrov, a digital manager at pCloud, stated that apps can retain, utilize, or sell many types of personal data, including browsing history, location, financial details, contact information, and fitness levels. Given its staggering 1 billion monthly active users, it is concerning that Instagram is a central platform for disseminating a substantial volume of personal data belonging to its oblivious users. Walker (2023) adds that regarding first-party usage, Instagram, a photo-sharing app owned by Facebook, is a prominent violator as it tracks user data to gain insights into app usage and provides suggestions for enhancement. Instagram ranks second in data collection for internal usage, with 86% of user data being utilized within the company, trailing only its parent company. Instagram collects a range of information comparable to what it shares with third parties and encompasses Apple's "other data" category.

Meta's parent platforms and targeted advertising

Considering the growing privacy concerns, it is natural that an increasing number of social media users are questioning how online platforms handle and utilize their supplied data. Facebook's recent admission that its Messenger app stored call and text logs of Android users who consented to sharing their contact list prompts us to consider how other similar social media platforms handle the data they are granted access to (Langone, 2018; McMillan, 2018). Dangerfield (2023) explains how Facebook uses targeted ads to track users' data online. Targeted adverts utilize your browser's data to enhance marketing efforts by tailoring them to your specific preferences and interests. Advanced algorithms analyze your website visits and searches over some time to anticipate your preferences and display advertisements that align with your interests. We have all experienced

the situation. If you are browsing the internet for a camera, a pair of shoes, or a kitchen gadget, you may see an advertisement for the same item appearing promptly on Facebook, YouTube, or your web browser. If you are looking for a trip to the Bahamas, you may notice increased advertisements from airlines and swimwear brands. The customized advertisements are generated based on cookies and an IP address. Cookies are digital files stored in your web browser that record and store information about your online activities and searches. An IP address functions similarly to a residential address, as it indicates the user's geographical location. The equilibrium between two entities is what provides advertisers with the necessary data.

Like many other social networks, Instagram collects and stores user data primarily to personalize advertisements displayed on your feed. These ad targeting adjustments are based on various data types, including your account information, usage patterns, and location (Burgess, 2020; Eg et al., 2023). However, it is important to note that your data is not the sole factor influencing the ads you see. Instagram also gathers similar data from a wide range of users and employs it to optimize the timing and placement of specific ads. Moreover, Instagram automatically utilizes facial recognition data to automatically identify your presence in photos (Dwivedi et al., 2021; Sprout Social, 2023). The additional data gathered by Instagram serves multiple purposes, such as conducting strategic market research, facilitating direct communication with users, and addressing any suspected misuse of the platform (Jones, 2023). Janssen (2023) provides insights into the phenomenon of feeling observed or stalked on Instagram in the context of personalized advertisements. The experience is articulated as individuals browsing the internet for specific products, such as headphones, and subsequently encountering targeted advertisements for these products upon accessing Instagram. The sense of being observed arises from the smilingly tailored nature of these advertisements, leading to a perception of unseen surveillance. This practice is attributed to Instagram's revenue generation model, which relies heavily on the sale of personalized advertisements. The significant financial implications of this model arr highlighted, with Instagram's advertising revenue demonstrating substantial growth over the years. For instance, in 2019, Instagram's advertising income in the United States exceeded $16 billion, this rose to over $50 billion in 2023, and is projected to rise further to $59 billion in 2024 (Iqbal, 2024; Zote, 2024).

Terms and conditions when signing up on social media

Terms and conditions establish the connection between social media companies and their users. Nevertheless, these legal agreements are often lengthy and written in complicated language. It raises doubts regarding user comprehension of these terms and conditions and their awareness of the potential outcomes of participating in such a network (Schneble et al., 2021; Stasi, 2019). When people decide to join a service, they usually agree by reading or quickly going through

the terms and conditions and clicking the agree button. However, these terms and conditions are lengthy and in complex legal jargon. This makes it unclear whether users, especially young people and teenagers, fully grasp the meaning of these terms or understand the potential repercussions of joining a network (Ducato, 2020; Mladinić et al., 2021). While most platforms offer their services for free, users often have to accept a set of conditions with limited privacy choices to access these services (Schneble et al. 2021). Koebert (2023) observes that social media has become an integral aspect of contemporary existence, as statistics indicate that a staggering 58% of the global population, equivalent to 4.6 billion individuals, presently engage with at least one social media platform. Billions of individuals are dedicating countless hours to engaging in activities such as posting, scrolling, liking, and commenting on social media sites, with a growing number of people joining these platforms daily.

Social media platforms possess the authority to utilize the content you share and continuously gather data from various sources, which you may need to be aware of (Stasi, 2019; Yaqub & Alsabban, 2023). For instance, Facebook can access information from all devices where its services are installed or accessed. Depending on the permissions granted to Facebook, it can collect data like device location obtained through GPS, Bluetooth, or Wi-Fi signals (Sapiezynski et al., 2019; Van Hoboken & Fathaigh, 2021). Additionally, it may gather details such as the name of your mobile provider, internet service provider, language, and time zone, as specified in its data policy. Similarly, X (formerly Twitter) obtains comparable metadata and can track users' locations even if their location services are disabled. This may be achieved by utilizing publicly broadcasted information from the user's wireless access point, such as a MAC Address, to estimate their approximate location, as indicated on Twitter's website (Khader & Karam, 2023; Ndinojuo & Ihejirika, 2018; Nguyen et al., 2022). Also, both platforms accumulate data about users from third-party websites that employ these social media services. For instance, if you visit a website with a "like" button or a site utilizing Facebook's advertising service, the social media company acquires data about your interactions with that site. Brad Frazer, an Internet IP and IT lawyer at Hawley Troxell, emphasized that users relinquish certain rights to their big data by accepting the terms of service and clicking on the "I agree" button (Dwivedi et al., 2021; Thompson, 2015).

Methodology

The survey research design was employed to conduct the investigation. This involves selecting a representative sample from the population to gather data on their characteristics, which can be generalized to the entire population. The survey method is an appropriate approach to obtain information on the level of awareness of the study group (Liao, 2023; Mishra et al., 2023). The population of this study comprises all current undergraduate students enrolled in the three campuses of the University of Port Harcourt (Choba, Abuja, and Delta). According to the Office

of the Registrar, University of Port Harcourt, the total number of registered undergraduate students at the university is 37,893. The large size of the population led to the utilization of the Taro Yamane statistical formula to determine the sample size for the study (Yamane, 1973). The formula is stated as follows:

$$n = \frac{N}{1=N(e)^2}$$

Where:
n = sample size
N = population size
e = the level of precision (degree of variability of 0.5)
Thus: substituting the values in the equation yields

$$n = \frac{37,893}{1+37,893(0.05)^2}$$

$$n = \frac{37,893}{1+37,893(0.0025)}$$

$$n = \frac{37,893}{95.7325}$$

n = 395.8, the sample size for this survey was approximated to 396 respondents.

The instrument used to gather data from the respondents is the web-based questionnaire using Google Form. The questionnaire was designed in unison with the research questions to maintain alignment between the research and survey questions. This is crucial for achieving clear, reliable results for easy and swift data analysis and comparison. The instrument consists of two sections (section A and section B), with section A containing four questions on the respondents' demographic information and section B consisting of 31 questions, for which respondents were expected to provide appropriate answers. Questions 1 – 6 of section B of the questionnaire cover research question 1, questions 6 – 11 cover research question 2, questions 12 – 16 cover research question 3, and questions 17 – 31 cover research question 4, respectively. The items on the questionnaire were structured using a four-point Likert rating scale made up of Strongly Agree (SA) = 4-point, Agree (A) = 3-point, Disagree (D) = 2-point and Strongly Disagree (SD) = 1-point and, Very high level= 4, high level = 3, Low level = 2 and Very low level= 1. Data employed the use of the mean and criterion mean. A mean score below the criterion of 2.5 was rejected while mean score from 2.5 upwards was accepted. The criterion mean is calculated thus: Criterion mean = 4+3+2+1 = 10/4 = 2.5.

The researcher's supervisor was given a copy of the measuring instrument (questionnaire), including the research objectives and questions. This was done to have the questionnaire undergo proper content and face review to ensure validity. To ensure the reliability of the study, several measures were implemented; first, a pilot test of the questionnaire was conducted with a small group of similar

participants to identify and correct any ambiguous questions. Internal consistency was assessed using Cronbach's alpha, with a value of 0.7 or higher indicating acceptable reliability, the results gave 0.72 as supported by Taber (2018) and Bujang et al. (2018). Test-retest reliability was ensured by administering the same questionnaire to the same group of participants at two different points in time and calculating the correlation between the two sets of responses (Kennedy, 2022; McCrae et al., 2011). Additionally, split-half reliability was examined by dividing the questionnaire into two halves and comparing the scores, ensuring a high correlation between them; these steps were collectively implemented to ensure that the research instrument provided consistent and stable results, enhancing the overall reliability of the study. Data for this research was collected by administering the web-based questionnaire to respondents (undergraduate students of the University of Port Harcourt). Descriptive statistics (including frequencies and percentages) and explanatory notes were employed during data analysis to determine the extent of awareness of personal data protection among Facebook and Instagram users.

Results

This section discussed the data gathered and findings from copies of questionnaires retrieved from the currently registered undergraduate students of the University of Port Harcourt, Nigeria. A total of 396 copies of the questionnaire were administered, and 124 responses were retrieved, representing a 31% success rate. The low retrieval rate was primarily attributed to the time constraints faced by the researchers, stemming from the need to adhere to stringent timelines and project deadlines. The demanding schedule imposed limitations on the outreach and engagement efforts, as there was a pressing requirement to collect data within a compressed timeframe. This time constraint not only impacted the researchers' ability to deploy the questionnaire effectively but also restricted the duration available for potential respondents to participate. This, however, did not negatively affect the overall results as the findings provided a glimpse into the awareness levels of social media users of privacy and personal data on Facebook and Instagram. This study utilized a 90% confidence level; this was chosen to balance precision and certainty, providing narrower confidence intervals for more precise estimates while accepting a 10% chance that the true population parameter might fall outside these intervals, it is deemed appropriate given the practical time constraints and the exploratory nature of the research.

Demographic information of the respondents

The demographic characteristics illustrated the distribution of respondents' categories in relation to gender, age range, level of study and faculty of the students that completed the survey.

Demographics	Variables	Frequency	Percent
Gender	Female	87	70.2
	Male	36	29.0
	Rather Not Say	1	0.8
Age	18-24	98	79
	25-34	26	21
	35-44	-	-
	45-above	-	-
Level of Study	100 level	6	4.8%
	200 level	16	12.9%
	300 level	24	19.4%
	400 level	65	52.4%
	500 level	13	10.4%
	600 level	-	-
Faculty of Study	Humanities	61	49.2%
	Engineering	13	10.5%
	Science	13	10.5%
	SSLT*	7	5.6%
	Management	5	4.0%
	Education	6	4.8%
	Law	2	1.6%
	Agriculture	3	2.4%
	Social Sciences	3	2.4%
	Basic Medical Sciences	5	4.0%
	Clinical Sciences	3	2.4%
	Pharmaceutical Sciences	3	2.4%
	Total	124	100%

SSLT – School of Science Laboratory Technology

Table 1. Gender of respondents

Data in Table 1 show that most respondents are females, while 0.8% preferred not to mention gender. Most of the respondents' 98 (79.0%) were under the age range of 18 – 24, indicating the ages typically associated with students. Ages above 35 recorded no entries, showing that most people of that age range are expected to have completed undergraduate studies. A majority of the respondents were 400-level students, with a 52.4% response rate; the lowest response was from 100-level students, who had 4.8%, and 600-level students had zero response. Most respondents, comprising 61 individuals (49.2% response rate), were from the Faculty of Humanities. The lowest response rate was observed in two faculties,

namely the Faculty of Clinical Sciences and the Faculty of Pharmaceutical Sciences, with 3 (2.4%) response rates each.

Research Question one: What is the awareness level of personal data protection among Facebook and Instagram Users?

S/N	Items	SA 4	A 3	D 2	SD 1	Total	Mean (X)	Decision
1	I am aware of the importance of protecting my personal data while using Facebook.	62 248	60 180	2 4	- -	124 432	3.5	Agreed
2	I am aware of the importance of protecting my personal data while using Instagram.	64 256	58 174	2 4	- -	124 434	3.5	Agreed
3	I understand the potential risks associated with sharing my personal information on Facebook and Instagram.	68 272	56 168	- -	- -	124 440	3 .5	Agreed
4	I am knowledgeable about the privacy settings and options available to protect my personal data on Facebook and Instagram.	56 224	59 177	8 16	1 1	124 418	3.4	Agreed
5	I am aware of my rights regarding my personal data on Facebook and Instagram, including the ability to control and access my data.	41 164	70 210	12 24	1 1	124 399	3.2	Agreed
6	I have read the user privacy statements of Facebook and Instagram.	27 108	68 204	4 8	25 25	124 345	2.7	Agreed
		CUMULATIVE				411.3	3.3	Agreed

Table 2. Mean (x) analysis on the awareness level of personal data protection among Facebook and Instagram Users

Based on the data presented in Table 2, it is evident that a significant majority of the respondents express awareness and understanding of the principles of personal data protection on the social media platforms Facebook and Instagram. Items 1, 2, 3, 4, 5, and 6 collectively indicate a consensus among the respondents regarding their awareness of the importance of safeguarding personal data while using these platforms. This alignment with the importance of personal data protection reflects a heightened consciousness among the respondents about preserving their privacy and controlling the dissemination of their personal information in the digital sphere. The clear agreement across these items emphasizes a widespread acknowledgment of the need for vigilance regarding personal data security on Facebook and Instagram, highlighting the relevance of this issue within the user community.

Research Question two: How many Users have taken precautionary measures to protect their personal data on Facebook and Instagram?

S/N	Items	SA 4	A 3	D 2	SD 1	Total	Mean (X)	Decision
7	I actively review and adjust my privacy settings on Facebook and Instagram to protect my personal data	27 108	68 204	25 50	4 8	124 370	3.0	Agree
8	I am careful about the amount of personal information I share on Facebook and Instagram	61 224	61 183	2 4	- -	124 431	3.5	Agree
9	I make use of strong unique passwords and enable two-factor authentication on both Facebook and Instagram.	61 244	52 156	9 18	2 2	124 400	3.2	Agreed
10	I am aware of the potential risks associated with third-party applications and carefully consider their access to my personal data on Facebook and Instagram	52 208	70 210	1 2	1 1	124 421	3.4	Agreed
11	I educate myself about the latest privacy features and settings offered by both Facebook and Instagram, and make use of them to protect my personal data	30 120	63 189	27 54	4 4	124 367	3.0	Agreed
		CUMULATIVE				399.6	3.2	Agreed

Table 3. Mean (x) analysis on the number of users who have taken precautionary measures to protect their personal data on Facebook and Instagram users

According to the data in Table 3, many respondents have taken aggressive steps to protect their personal information on the social media sites Facebook and Instagram. The respondents' agreement on securing their personal data on these sites is demonstrated by items 7, 8, 9, 10, and 11. The collective agreement stresses the respondents' strong feelings of personal responsibility and awareness in actively controlling their privacy and security settings. Their resolute efforts demonstrate an awareness of the possible hazards linked to internet data exposure and a dedication to reducing these risks through proactive measures. The respondents' agreement with these items demonstrates their proactive and vigilant approach to safeguarding the confidentiality and security of their personal information on Facebook and Instagram.

Research Question three: What are the reasons for the precautionary measures taken by Users to protect personal data?

S/N	Items	SA 4	A 3	D 2	SD 1	Total	Mean (X)	Decision
12	I take precautionary measures because they are important for the protection of my personal data	43 172	71 213	10 10	- -	124 405	3.3	Agreed
13	I believe that protecting my personal data helps prevent identity theft and fraud	65 260	59 177	- -	- -	124 437	3.5	Agreed
14	I take precautionary measures to protect my personal data because I want to have control over my privacy and the information I share	51 204	70 210	3 6	- -	124 420	3.4	Agreed
15	I am more comfortable to share personal information when I know that I have already taken precautionary measures	31 124	57 171	31 61	5 5	124 361	3.0	Agreed
16	I have implemented precautionary measures because it enables me to maintain privacy and confidentiality	42 168	71 213	11 22	- -	124 502	4.0	Agreed
		CUMULATIVE				425	3.4	Agreed

Table 4. Mean (x) analysis on the reasons for the precautionary measures taken by Users to protect personal data

Table 4 data indicates that most respondents have proactively protected their personal information and privacy on Facebook and Instagram. The respondents' collective agreement highlights their acknowledgment of the potential risks associated with identity theft, fraud, and the unauthorized use of their personal information. The respondents demonstrate responsibility and understanding by agreeing to take precautionary measures to preserve their privacy and personal data online. Their proactive approach delineates a commitment to minimizing the risks associated with unauthorized access and misuse of their personal information, emphasizing the significance of privacy and data security within the context of Facebook and Instagram usage.

Research Question four: What are the agencies and regulatory bodies responsible for personal data protection?

S/N	Items	SA 4	A 3	D 2	SD 1	Total	Mean (X)	Decision
17	I know that the National Information Technology Development Agency (NITDA) is a personal data protection and regulatory Agency in Nigeria.	9 36	62 186	49 98	4 4	124 324	2.6	Agreed
18	I have contacted the NITDA concerning privacy issues in the past.	2 8	9 27	84 168	29 29	124 232	1.9	Disagreed
19	I know someone who has contacted the NITDA concerning privacy issues in the past.	4 16	10 30	78 156	32 32	124 234	1.8	Disagreed
20	I know that the Nigerian Communications Commission (NCC) is a personal data protection and regulatory Agency.	15 60	57 171	47 94	5 5	124 330	2 .7	Agreed
21	I have contacted the NCC concerning privacy issues in the past.	5 20	9 27	78 156	28 28	124 234	1.9	Disagreed
22	I know someone who has contacted the NCC concerning privacy issues in the past.	5 20	13 39	78 156	28 28	124 243	2.0	Disagreed
23	I know that the National Identity Management Commission (NIMC) is a personal data protection and regulatory Agency in Nigeria.	25 100	64 192	28 56	7 71	124 419		Disagreed
24	I have contacted the NIMC concerning privacy issues in the past.	9 36	29 87	58 116	28 28	124 264	2.2	Disagreed
25	I know someone who has contacted the NIMC concerning privacy issues in the past.	11 44	17 51	70 140	26 26	12 261	2.1	Disagreed
26	I know that the Economic and Financial Crimes Commission (EFCC) is a personal data protection and regulatory agency.	25 100	56 168	33 66	10 10	124 344	2.8	Agreed
27	I have contacted the EFCC concerning privacy issues in the past.	33 132	11 33	74 148	10 10	124 319	2.6	Agreed
28	I know someone who has contacted the EFCC	9	20	62	32	124	2.0	Disagreed

	concerning privacy issues in the past.	36	60	124	32	252		
29	I know that the Nigeria Data Protection Commission (NDPC) is a personal data protection and regulatory agency.	10 40	51 153	42 84	21 21	298	2.3	Disagreed
30	I have contacted the NDPC concerning privacy issues in the past.	4 16	11 33	78 156	31 31	124 236	1.9	Disagreed
31	I know someone who has contacted the NDPC concerning privacy issues in the past.	6 24	8 24	86 172	24 24	124 244	2.0	Disagreed
		CUMULATIVE				282	2.3	Disagreed

Table 5. Mean (x) analysis on the identification of the agencies and regulatory bodies responsible for personal data protection

Table 5 presents the survey data regarding respondents' knowledge and interactions with various regulatory agencies related to personal data protection in Nigeria. Most respondents agreed that Nigeria's National Information Technology Development Agency (NITDA) and the Economic and Financial Crimes Commission (EFCC) are personal data protection and regulatory agencies, indicating relatively high awareness of these organizations. On the other hand, there was a larger disagreement among respondents regarding their knowledge of the Nigeria Data Protection Commission (NDPC), the National Identity Management Commission (NIMC), and the Nigerian Communications Commission (NCC) as personal data protection and regulatory agencies. The data shows that a relatively low number of respondents had previously contacted the regulatory agencies concerning privacy issues, with a higher level of disagreement.

Discussions

Research Question one: What is the awareness level of personal data protection among Facebook and Instagram Users?

Items 1, 2, 3, 4, 5, and 6 in Table 2 were used to answer this research question. Respondents in item 1 confirmed that they know the importance of protecting their personal data while using Facebook. Respondents in item 2 agreed that they are aware of the importance of protecting their personal data while using Instagram. The respondents in item 3 also agreed that they understand the potential risks of sharing their personal information on Facebook and Instagram. This view is supported by the Privacy Calculus Theory, as stated by various scholars (Fu et al., 2023; Laufer & Wolfe, 1977; Meir & Krämer, 2022; Princi & Krämer, 2020). The theory assumes people weigh perceived risks and benefits before disclosing personal infor-

mation. The findings agree with the authors (Gogus & Saygın, 2019; Külcü & Henkoğlu, 2014) looking at privacy in Turkey, and Rainie (2018). Madden (2012) and Benisch et al. (2011) from a North American perspective that users consider data previous a serious issue, compared to Asia users who agreed that online data may not be safe, but so long as some restrictions are in place, they can live with the consequences (Das, 2022; Ee, 2023).

In item 4, the respondents affirmed that they are knowledgeable about the privacy settings and options available to protect personal data on Facebook and Instagram. Then, in item 5, the respondents agreed that they are aware of their rights regarding personal data on Facebook and Instagram, including the ability to control and access their data. This result was backed up by Warren (2022), who said, "The dot com boom brought about an exponential increase in the amount of data created and stored across the internet. As a result, the security of personal data shared online has become a real national concern, with state actors, organizations, and hackers constantly attempting to exploit information of data subjects that should be handled ethically for commercial or malicious purposes. Most of the data the world has produced are personal data (or data that can be traced back to specific individuals)". Respondents in item 6 agreed that they had read the User privacy statements of Facebook and Instagram. This result was in total agreement with the postulations of Schneble et al. (2021), which say that when people decide to join a service, they usually agree by reading or quickly going through the terms and conditions and clicking the agree button. However, these terms and conditions are lengthy and in complex legal jargon. This makes it unclear whether users, especially young people and teenagers, fully grasp the meaning of these terms or understand the potential repercussions of joining a network.

Research Question two: How many Users have taken precautionary measures to protect their personal data on Facebook and Instagram?

Items 7, 8, 9, 10, and 11 in Table 3 were used to answer this research question. In item 7, the respondents affirmed that they actively review and adjust privacy settings on Facebook and Instagram to protect their personal data. This result contrasts with Koebert's (2023) view that, while the terms of service for social media sites and apps are available for review, how many people look at them before signing up? More importantly, how many could understand them if they did? Terms of service for all sorts of things are relatively easy to read and understand. They are full of page after page of legalese and jargon that is inaccessible to the average person. Regarding social media, these statements are just as confusing". In item 8, the respondents confirmed that they were careful about how much personal information they share on Facebook and Instagram. In item 9, the respondents agreed to use strong, unique passwords and enable two-factor authentication on Facebook and Instagram. In item 10, the respondents agreed that they know the potential risks associated with third-party applications and carefully consider their access to Users' data on Facebook and Instagram. This result supported the views of West

and Zuboff (2019), who asserted that self-disclosure will be more likely in a particular situation if a person perceives high benefits in a particular case because the benefits outweigh the risks. Contrarily, if this person anticipates higher risks with disclosure compared to other situations, information revelation will be less likely in this particular situation due to an overweight of the privacy risk perception. In item 11, the respondents affirmed that they educate themselves about the latest privacy features and settings offered by Facebook and Instagram and use them to protect their personal data.

Research Question three : What are the reasons for the precautionary measures taken by Users to protect personal data?

Items 12, 13, 14, 15, and 16 in Table 4 were used to provide answers to this research question. In item 12, the respondents affirmed that they take precautionary measures because they are important for protecting personal data. This result is supported by Warren (2022); as technology progresses and becomes more advanced, we must also acknowledge the potential hazards linked to digital privacy breaches, cybersecurity threats, and the responsible and ethical handling of data. Item 13 shows that Respondents believe protecting their personal data helps prevent identity theft and fraud. In item 14, respondents agree that one of the reasons they take precautionary measures is to protect their personal data because they want to have control over their privacy and the information they share. In item 15, Respondents affirmed that they are more comfortable sharing personal information when they know they have taken precautionary measures to protect their personal data. This result is supported by Crossman (2020). The Social exchange theory is a framework that helps us understand society as a series of interactions between individuals, where the anticipated rewards and punishments influence our actions. This theory suggests that we evaluate the potential outcomes of our interactions using a cost-benefit analysis, whether consciously or subconsciously. Item 16 Respondents confirmed that they have implemented precautionary measures because it enables them to maintain privacy and confidentiality.

Research Question four: What are the agencies and regulatory bodies responsible for personal data protection?

Items 17–31 in Table 5 were used to answer the research question 4. In item 17, the respondents affirmed that Nigeria's National Information Technology Development Agency (NITDA) is a personal data protection and regulatory agency. Item 18 show that respondents disagreed that they had contacted the NITDA concerning privacy issues. In item 19, respondents disagreed that they knew someone who had contacted the NITDA concerning privacy issues. In item 20, the respondents affirmed that the Nigerian Communications Commission (NCC) is a personal data protection and regulatory agency. In item 21, the respondents disagreed that they had contacted the NCC concerning privacy issues. Respondents

in item 22 also disagreed that they knew someone who had contacted the NCC concerning privacy issues. Item 23 showed respondents agreed that the National Identity Management Commission (NIMC) is Nigeria's personal data protection and regulatory agency. In item 24, the respondents disagreed that they had contacted the NIMC concerning privacy issues. Respondents in item 25 also disagreed that they knew someone who had contacted the NIMC concerning privacy issues. Item 26 shows respondents agreed that the Economic and Financial Crimes Commission (EFCC) is a personal data protection and regulatory agency. In item 27, the respondents agreed that they had contacted the EFCC concerning privacy issues. Respondents in item 28 disagreed that they knew someone who had contacted the EFCC concerning privacy issues in the past. Item 29 shows that Respondents disagreed that they knew that the Nigeria Data Protection Commission (NDPC) is a personal data protection and regulatory agency. In item 30, the respondents disagreed that they had contacted the NDPC concerning privacy issues. Respondents in item 31 also disagreed that they knew someone who had contacted the NDPC concerning privacy issues in the past. These results were supported by Lambo et al. (2023) in a careful review of the principal data protection legislation, which included a list of the agencies and regulatory bodies as mentioned in Table 5. Despite the list provided, users were still unable to identify the agencies. The study's results indicate that social media users possess a general understanding of personal data protection but lack awareness of the specific regulatory authorities that are significant. This emphasizes a crucial deficiency in the current awareness programs and indicates a necessity for more focused education (Ducato, 2020; Mladinić et al., 2021). The authors suggest that the agencies concerned should conduct instructional workshops and provide easily available guidelines that guide internet users on the privacy of online data.

Conclusion

This research was conceptually and theoretically designed on the awareness of personal data protection among Facebook and Instagram users. This study effectively evaluated the awareness level of personal data protection among Facebook and Instagram Users, the number of Users who have carefully taken precautionary measures to protect their personal data on Facebook and Instagram, the reasons why Users have taken such precautionary measures, and the identification of the agencies and the regulatory bodies responsible for personal data protection. The following are the key findings from the research:

- Students know the importance of personal data protection on both Facebook and Instagram.
- Students are knowledgeable about the potential risks associated with personal data.

- Students took precautionary measures to protect their personal data and have reasons for taking such measures.
- Students need training and proper provision of information regarding the protection of personal data, and more awareness campaigns should be held for proper introduction and identification of the Agencies and regulatory bodies responsible for the protection of personal data.

This study has elucidated the diverse degrees of consciousness regarding the safeguarding of personal data among the undergraduate students of the University of Port Harcourt. It was clear that although several students had a strong grasp of the need of safeguarding their personal information, a significant section of the student population might have benefitted from additional instructional and awareness campaigns. In order to prepare for the future, it is crucial for the University to prioritize the implementation of focused campaigns and educational programs. These initiatives should aim to improve students' understanding and awareness of personal data protection on social media. This can be achieved by providing students with the necessary information and resources, as well as fostering a secure and privacy-conscious environment within the University of Port Harcourt student community.

The study's limitations include several factors that influenced the research process and outcomes; they are explained further. The study faced a low response rate leading to data collection challenges due to a limited response from the web-based questionnaire. The cautious approach of students towards personal information sharing resulted in a low response rate, impacting the representativeness of the data. Respondents also mentioned having trust issues with external links. Their skepticism and reluctance to click on links in the questionnaire stemmed from genuine concerns about online scams. Some participants' expressed having been previously targeted by fraudulent activities disguised as academic surveys, leading to a hesitancy to engage with similar requests. The low retrieval rate of the research instrument, constituting only 31% of the sample size, indicates a significant limitation in the representativeness and generalizability of the findings. The reduced participation compromised the breadth and depth of the data collected. The constraints experienced likely impacted the validity and reliability of the study, raising questions about the accuracy and comprehensiveness of the gathered data. However, the findings provided some insight into the awareness levels of privacy and personal data on Facebook and Instagram, and by extension, social media platforms. Finally, the limited response rate may hinder the generalizability of the findings, as the sample may not fully represent the broader population, creating potential biases in the results. The following recommendations are proposed after analyzing the data and discussing the findings:

1. Organize specific educational workshops to promote understanding of the pertinence of safeguarding personal data on social media platforms.

2. The University of Port Harcourt Administration should include personal data protection awareness in its orientation programs and student events.
3. Create easily accessible materials and guidelines on the University of Port Harcourt Portal designed for Facebook and Instagram users, outlining the best methods for protecting personal data.
4. Set up a system for reporting potential data breaches and offer assistance to affected users, as well as organising campaigns for the proper identification of the Regulatory bodies and Agencies responsible for the protection of personal data.

The findings highlight the immediate need for enhanced awareness and educational campaigns to safeguard users' personal data (Mohammad et al., 2022), particularly on Facebook and Instagram; an important revelation is the exposition of the different levels of awareness of data protection rules and practices among undergraduate students at the University of Port Harcourt, focusing on its wider significance. These support the implementation of initiatives such as educational workshops, integrating data protection awareness into educational programs and the development of east-to-read guidelines for social networking sites users. The study emphasizes the significance of deploying strong reporting systems for suspected data breaches and promoting cooperation and data sharing with regulatory agencies to improve the data protection legislation.

Acknowledgment

The authors would like to thank colleagues who provided moral support and guidance in this study and also appreciate the reviewers of this paper for their valuable advice.

References | Список литературы

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Barrett-Maitland, N., & Lynch, J. (2020). Social Media, Ethics and the Privacy Paradox. In C. Kalloniatis & C. Travieso-Gonzalez (Eds.), *Security and Privacy From a Legal, Ethical, and Technical Perspective*. IntechOpen. https://doi.org/10.5772/intechopen.90906

Barth, S., De Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. (2011). Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing*, 15(7), 679–694. https://doi.org/10.1007/s00779-010-0346-0

Bhageshpur, K. (2019, November 15). *Data is the new oil—And that's a good thing*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=788fcad87304

Bhasin, H. (2022, January 7). *Awareness—Definition, meaning and examples*. Marketing91 Academy. https://www.marketing91.com/awareness/

Bujang, M. A., Omar, E. D., & Baharum, N. A. (2018). A Review on Sample Size Determination for Cronbach's Alpha Test: A Simple Guide for Researchers. *Malaysian Journal of Medical Sciences*, 25(6), 85–99. https://doi.org/10.21315/mjms2018.25.6.9

Burgess, M. (2020). *How to stop Instagram** from tracking everything you do*. Wired. https://www.wired.co.uk/article/instagram-story-ads-privacy-delete

Butori, R., & Lancelot Miltgen, C. (2023). A construal level theory approach to privacy protection: The conjoint impact of benefits and risks of information disclosure. *Journal of Business Research*, 168, 114205. https://doi.org/10.1016/j.jbusres.2023.114205

Coronado-Maldonado, I., & Benítez-Márquez, D. (2023). Emotional intelligence, leadership, and work teams: A hybrid literature review. *Heliyon*, 9(10), e20356. https://doi.org/10.1016/j.heliyon.2023.e20356

Crocetti, P., Peterson, S., & Hefner, K. (2023). *What is data protection and why is it important*. Tech Target. https://www.techtarget.com/searchdatabackup/definition/data-protection

Crossman, A. (2020, January 14). *Understanding social exchange theory*. ThoughtCo. https://www.thoughtco.com/social-exchange-theory-3026634

Dangerfield, K. (2023). *Facebook**, Google and others are tracking you. Here's how to stop targeted ads*. https://globalnews-ca.cdn.ampproject.org/v/s/globalnews.ca/news/4110311/

Das, M. C. (2022). Data Privacy on the Internet: A Study on Awareness and Attitudes among the Students of the University of Chittagong in Bangladesh. *Advances in Journalism and Communication*, 10(2), 70–80. https://doi.org/10.4236/ajc.2022.102006

Dennis, M. (2019). *Facebook** and Instagram**: Privacy challenges*. https://www-coursebb-com.cdn.ampproject.org/v/s/www.coursebb.com/2019/03/05/

Dixon, S. J. (2023). *Global social networks ranked by number of users* 2023. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review*, 37, 105412. https://doi.org/10.1016/j.clsr.2020.105412

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, 59, 102168. https://doi.org/10.1016/j.ijinfomgt.2020.102168

Ee, C. J. (2023). Analysis of privacy awareness among social media users in Malaysia. *Jurnal Pengajian Media Malaysia / Malaysian Journal of Media Studies*, 25(1), 67–80. https://doi.org/10.22452/jpmm.vol25no1.6

Eg, R., Demirkol Tønnesen, Ö., & Tennfjord, M. K. (2023). A scoping review of personalized user experiences on social media: The interplay between algorithms and human factors. *Computers in Human Behavior Reports*, 9, 100253. https://doi.org/10.1016/j.chbr.2022.100253

Eludu, S., Mbazie, S., & Ndinojuo, B.-C. (2016). Application of ICT in television broadcasting: A study of NTA Port Harcourt. *International Journal of Science Inventions Today*, 5(2), 169–182.

Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11–36. https://doi.org/10.1093/idpl/ipz026

Fu, J., Zhang, J., & Li, X. (2023). How do risks and benefits affect user' privacy decisions? An event-related potential study on privacy calculus process. *Frontiers in Psychology*, 14, 1052782. https://doi.org/10.3389/fpsyg.2023.1052782

Gazi, T. (2020). Data to the rescue: How humanitarian aid NGOs should collect information based on the GDPR. *Journal of International Humanitarian Action*, 5(1), 1–7. https://doi.org/10.1186/s41018-020-00078-0

Gielens, K., & Steenkamp, J. E. (2019). Branding in the era of digital (dis)intermediation. *International Journal of Research in Marketing*, 36(3), 367–384. https://doi.org/10.1016/j.ijresmar.2019.01.005

Gogus, A., & Saygın, Y. (2019). Privacy perception and information technology utilization of high school students. *Heliyon*, 5(5), e01614. https://doi.org/10.1016/j.heliyon.2019.e01614

Hill, M., & Swinhoe, D. (2022, November 8). *The 15 biggest data breaches of the 21st century*. CSO. https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

Ihejirika, W., Mbazie, S., & Ndinojuo, B. (2015). Use of social media by political parties in Nigeria: An analysis of Facebook** and Twitter. *International Journal of Communication: An Interdisciplinary Journal of Communication Studies*, 16(9), 16–30.

Iqbal, M. (2024, July 8). Instagram** revenue and usage statistics (2024). *Business of Apps*. https://www.businessofapps.com/data/instagram-statistics/

Irwin, L. (2022, June 11). *The GDPR: What exactly is personal data?* IT Governance. https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data

Ja'han, J. (2023). *Privacy rules are Meta's biggest obstacle to world domination*. MSNBC. https://www.msnbc.com.cdn.ampproject.org/v/s/www.msnbc.com/msnb/

Janssen, D. (2023, November 28). *What does Instagram** know about me*. VPNOverview. https://vpnoverview.com/privacy/social-media/what-does-instagram-know-about-me/

Jati, H. F., Darsono, S. N. A. C., Hermawan, T., Yudhi, W. A. S., & Rahman, F. F. (2019). Awareness and knowledge assessment of sustainable development goals among university students. *Jurnal Ekonomi & Studi Pembangunan*, 20(2), 163–175. https://doi.org/10.18196/jesp.20.2.5022

Jocelli, J. O. (2016). *Cookies policy and social media*. Janna Joceli Omena. https://thesocialplatforms.wordpress.com/2016/09/30/cookies-policy-and-social-media/

Kemp, S. (2023, February 13). *Digital 2023: Nigeria*. *Data Reportal*. https://datareportal.com/reports/digital-2023-nigeria

Kennedy, I. (2022). Sample Size Determination in Test-Retest and Cronbach Alpha Reliability Estimates. *British Journal of Contemporary Education*, 2(1), 17–29. https://doi.org/10.52589/BJCE-FY266HK9

Keskin, A. D., Kaytez, N., Damar, M., Elibol, F., & Aral, N. (2023). Sharenting syndrome: An appropriate use of social media? *Healthcare*, 11(10), 1359. https://doi.org/10.3390/healthcare11101359

Khader, M., & Karam, M. (2023). Assessing the effectiveness of masking and encryption in safeguarding the identity of social media publishers from advanced metadata analysis. *Data*, 8(6), 105. https://doi.org/10.3390/data8060105

King'ori, M. (2023, June 28). *Nigeria's new data protection act explained*. *Future of Privacy Forum*. https://fpf.org/blog/nigerias-new-data-protection-act-explained/

Koebert, J. (2023, August 24). *You'll need a college education to read the terms of service for these social media sites*. *All about Cookies*. https://allaboutcookies.org/social-media-terms-of-service

Külcü, Ö., & Henkoğlu, T. (2014). Privacy in social networks: An analysis of Facebook**. *International Journal of Information Management*, 34(6), 761–769. https://doi.org/10.1016/j.ijinfomgt.2014.07.006

Lajnef, K. (2023). The effect of social media influencers' on teenagers behavior: An empirical study using cognitive map technique. *Current Psychology*, 42(22), 19364–19377. https://doi.org/10.1007/s12144-023-04273-1

Lambo, J., Okolie, C., & Chukwuma, C. (2023). *Data protection laws and regulations in Nigeria*. https://iclg.com.cdn.ampproject.org/v/s/iclg.com/practice-areas/

Langone, A. (2018, March 26). *Facebook** admits it may collect data about your calls and text messages. Here's how to turn it off*. Time. https://time.com/5215274/facebook-messenger-android-call-text-message-data/

Lauer, D. (2021). Facebook's** ethical failures are not accidental; they are part of the business model. *Ai and Ethics*, 1(4), 395–403. https://doi.org/10.1007/s43681-021-00068-x

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Liao, C.-H. (2023). Exploring the Influence of Public Perception of Mass Media Usage and Attitudes towards Mass Media News on Altruistic Behavior. *Behavioral Sciences*, 13(8), 621. https://doi.org/10.3390/bs13080621

Lomas, N. (2021). *Facebook** accused of continuing to surveil teens for and targeting*. https://techcrunch-com.cdn.ampproject.org/v/s/techcrunch.com/2021/11/16/

London, M., Sessa, V. I., & Shelley, L. A. (2023). Developing Self-Awareness: Learning Processes for Self- and Interpersonal Growth. *Annual Review of Organizational Psychology and Organizational Behavior*, 10(1), 261–288. https://doi.org/10.1146/annurev-orgpsych-120920-044531

Lynskey, O. (2023). Complete and Effective Data Protection. *Current Legal Problems*, 76(1), 297–344. https://doi.org/10.1093/clp/cuad009

Lyons, K. (2023). *28 top social media platforms worldwide*. Semrush Blog. https://www.semrush.com/blog/most-popular-social-media-platforms/

Maddocks, J. (2023). Introducing an attitude-based approach to emotional intelligence. *Frontiers in Psychology*, 13, 1006411. https://doi.org/10.3389/fpsyg.2022.1006411

Majolo, M., Gomes, W. B., & DeCastro, T. G. (2023). Self-Consciousness and Self-Awareness: Associations between Stable and Transitory Levels of Evidence. *Behavioral Sciences*, 13(2), 117. https://doi.org/10.3390/bs13020117

Marcelline, M. (2023, May 14). *Facebook** fixes bug that sent friend requests if you looked at a profile*. PC Magazine. https://www.pcmag.com/news/meta-fixes-facebook-bug-that-sent-automatic-friend-requests

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. *Computer Law & Security Review*, 50, 105849. https://doi.org/10.1016/j.clsr.2023.105849

McCrae, R. R., Kurtz, J. E., Yamagata, S., & Terracciano, A. (2011). Internal Consistency, Retest Reliability, and Their Implications for Personality Scale Validity. *Personality and Social Psychology Review*, 15(1), 28–50. https://doi.org/10.1177/1088868310366253

McDermott, A. (2023, November 8). *Why safeguarding customer information has never been more critical*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/11/08/why-safeguarding-customer-information-has-never-been-more-critical/?sh=2d74748f59ef

McDonald, A. (2023). *Data protection privacy law*. Britannica. https://www.britannica.com/topic/data-protection

McMillan, R. (2018, March 26). *Facebook** logs text, call histories for some android users*. Wall Street Journal. https://www.wsj.com/articles/facebook-logs-text-call-histories-for-some-android-users-1522072657

Meier, Y., & Krämer, N. C. (2024). The Privacy Calculus Revisited: An Empirical Investigation of Online Privacy Decisions on Between- and Within-Person Levels. *Communication Research*, 51(2), 178–202. https://doi.org/10.1177/00936502221102101

Milligan, I. (2022). *The Transformation of Historical Research in the Digital Age* (1st ed.). Cambridge University Press. https://doi.org/10.1017/9781009026055

Mishra, M., Kushwaha, R., Gupta, N., Sinha, A., & Dwivedi, H. (2023). Survey data to evaluate consumer behaviour and consumption pattern of sustainable apparel: A study on consumer awareness level. *Data in Brief*, 49, 109350. https://doi.org/10.1016/j.dib.2023.109350

Mladinić, A., Puljak, L., & Koporc, Z. (2021). Post-GDPR survey of data protection officers in research and non-research institutions in Croatia: A cross-sectional study. *Biochemia Medica*, 31(3), 447–457. https://doi.org/10.11613/BM.2021.030703

Mohammad, T., Mohamed Hussin, N. A., & Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology. *Technology in Society*, 68, 101823. https://doi.org/10.1016/j.techsoc.2021.101823

Ndinojuo, B.-C., & Ihejirika, W. C. (2015). A review of Facebook** followership for political parties in Nigeria. *International Journal of Banking, Finance & Digital Marketing*, 1(1), 42–54.

Ndinojuo, B.-C., & Ihejirika, W. C. (2018). Nigerian political parties and their social media followership: Aftermath of 2015 general elections. *Media and Communication Currents*, 2(2), 39–58.

Nguyen, H. L., Tsolak, D., Karmann, A., Knauff, S., & Kühne, S. (2022). Efficient and Reliable Geocoding of German Twitter Data to Enable Spatial Data Linkage to Official Statistics and Other Data Sources. *Frontiers in Sociology*, 7, 910111. https://doi.org/10.3389/fsoc.2022.910111

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Nwagwu, W. E., & Akintoye, A. (2023). Influence of social media on the uptake of emerging musicians and entertainment events. *Information Development*, 026666692211511. https://doi.org/10.1177/02666669221151162

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook**. *South African Journal of Science*, 114(5/6), 5. https://doi.org/10.17159/sajs.2018/20170103

Obi, U. V. (2020, September 16). *Data privacy and data protection law in Nigeria*. Alliance Law Firm. https://alliancelawfirm.ng/data-privacy-and-data-protection-law-in-nigeria/

Oturu, D. (2019). *An overview of big data protection in Nigeria*. https://www.aelex.com/wp-content/uploads/2019/05/An-overview-of-Big-Data-and-data-protection-in-Nigeria-1-compressed.pdf

Pala, K. (2023). The interplay of indexicality between essence and meanings: An interconnection of experiences and memory. *Humanities and Social Sciences Communications*, 10(1), 556. https://doi.org/10.1057/s41599-023-02036-8

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, 9(4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007

Pretorius, A., & Plaatjies, B. O. (2023). Self-Awareness as a Key Emotional Intelligent Skill for Secondary School Principals' Leadership Toolkit. *Research in Educational Policy and Management*, 5(2), 52–74. https://doi.org/10.46303/repam.2023.9

Princi, E., & Krämer, N. C. (2020). Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices. *Frontiers in Psychology*, 11, 582054. https://doi.org/10.3389/fpsyg.2020.582054

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Rainie, L. (2018). *Americans' complicated feelings about social media in an era of privacy concerns*. The Pew Research Center. https://www.pewresearch.org/facttank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacyconcerns/

Sapiezynski, P., Stopczynski, A., Lassen, D. D., & Lehmann, S. (2019). Interaction data from the Copenhagen Networks Study. *Scientific Data*, 6(1), 315. https://doi.org/10.1038/s41597-019-0325-x

Sattin, D., Magnani, F. G., Bartesaghi, L., Caputo, M., Fittipaldo, A. V., Cacciatore, M., Picozzi, M., & Leonardi, M. (2021). Theoretical Models of Consciousness: A Scoping Review. *Brain Sciences*, 11(5), 535. https://doi.org/10.3390/brainsci11050535

Schneble, C. O., Favaretto, M., Elger, B. S., & Shaw, D. M. (2021). Social Media Terms and Conditions and Informed Consent From Children: Ethical Analysis. *JMIR Pediatrics and Parenting*, 4(2), e22281. https://doi.org/10.2196/22281

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.

Shubladze, S. (2023, May 27). *How to make use of the new gold: Data*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2023/03/27/how-to-make-use-of-the-new-gold-data/?sh=7e5653502bbf

Siegel, R. (2018, April 4). *Panera's data breach puts attention on risks of loyalty programs*. The Washington Post. https://www.washingtonpost.com/news/business/wp/2018/04/04/paneras-data-breach-puts-attention-on-risks-of-loyalty-programs/

Social media advertising: How it works and tips for success. (2023, May 2). *Sproutsocial*. https://sproutsocial.com/insights/social-media-advertising-strategy/

Solove, D. J. (2021). *Understanding Privacy*. Harvard University Press.

Stasi, M. L. (2019). Social media platforms and content exposure: How to restore users' control. *Competition and Regulation in Network Industries*, 20(1), 86–110. https://doi.org/10.1177/1783591719847545

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, 48(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Tang, Y., & Ning, X. (2023). Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems*, 165, 113881. https://doi.org/10.1016/j.dss.2022.113881

Thompson, C. (2015, May 20). *What you really sign up for when you use social media*. CNBC. https://www.cnbc.com/2015/05/20/what-you-really-sign-up-for-when-you-use-social-media.html

Tisserand, A., Philippi, N., Botzung, A., & Blanc, F. (2023). Me, Myself and My Insula: An Oasis in the Forefront of Self-Consciousness. *Biology*, 12(4), 599. https://doi.org/10.3390/biology12040599

Van Hoboken, J., & Fathaigh, R. Ó. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review*, 41, 105557. https://doi.org/10.1016/j.clsr.2021.105557

Venugeetha, Y., Rathod, R., & Kumar, R. (2022). Social networking sites in daily life: Benefits and threats. In S. Hiranwal & G. Mathur (Eds.), *Artificial Intelligence and Communication Technologies* (pp. 51–64). Soft Computing Research Society. https://doi.org/10.52458/978-81-955020-5-9-5

Vilić, V., & Radenković, I. (2015). Privacy Protection on Facebook**, Twitter and LinkedIn. *Proceedings of the International Scientific Conference – Synthesis* 2015, 735–738. https://doi.org/10.15308/Synthesis-2015-735-738

Walker, S. C. (2023, February 9). *Instagram** is sharing 79% of your personal data with third parties*. Cybernews. https://cybernews.com/privacy/instagram-is-sharing-79-of-your-personal-data-with-third-parties/

Warren, O. (2022, September 26). *The emergence and evolution of the Nigerian data protection regulation*. LinkedIn. https://www.linkedin.com/pulse/emergence-evolution-nigerian-data-protection-warren-oluwasanya

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, 58(1), 20–41. https://doi.org/10.1177/0007650317718185

Westin, A. F. (2003). *Privacy and freedom*. IG Publishing.

Yamane, T. (1973). *Statistics: An Introductory Analysis* (3rd ed.). Harper and Row.

Yaqub, M., & Alsabban, A. (2023). Knowledge Sharing through Social Media Platforms in the Silicon Age. *Sustainability*, 15(8), 6765. https://doi.org/10.3390/su15086765

Zote, J. (2024, Feb. 22).Instagram** statistics you need to know for 2024 [Updated]. *Sproutsocial*. https://sproutsocial.com/insights/instagram-stats/

** – A social network owned by "Meta", which is recognized as extremist in Russia