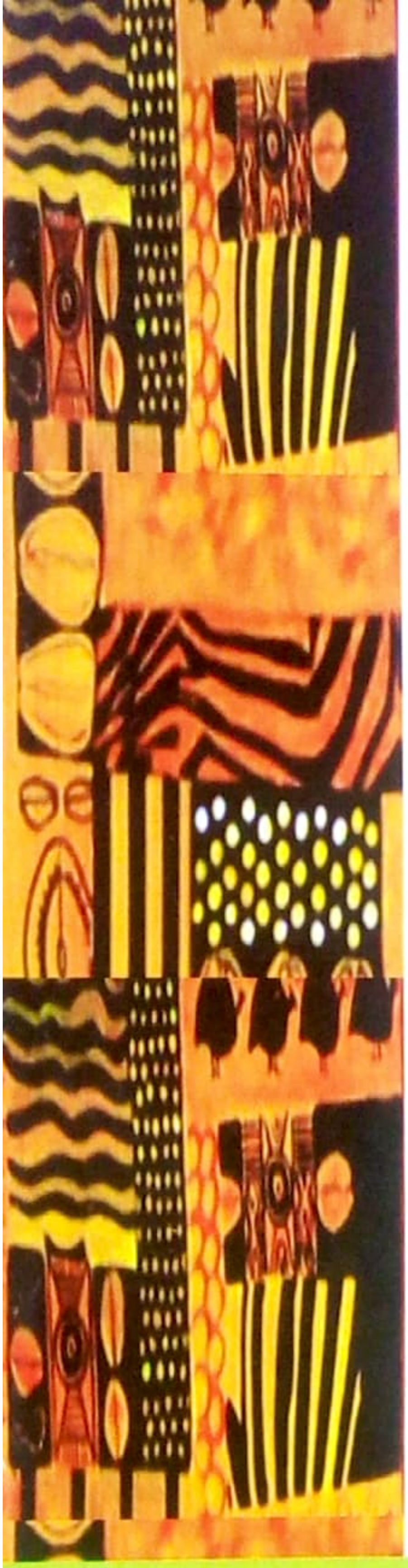

BENUE STATE UNIVERSITY

Scientia Liberatio Populorum

MAKURDI JOURNAL OF COMMUNICATION RESEARCH (MJCR)

VOL. 10 NO. 2

ISSN: 2141-050X

The Makurdi Journal Of Communication Research (mjcr) Is A Refereed Biannual International Journal That Publishes Original Papers On Human Communication Research, Theory And Practice

OCTOBER, 2023

WAR AGAINST THE 4TH ESTATE: USE OF SPYWARE AGAINST JOURNALISTS IN NIGERIA

Desmond Onyemechi Okocha, PhD
Department of Mass Communication,
Bingham University, Nigeria
Email: desmonddoo@yahoo.com

Ayuba John Ramadan
Department of Mass Communication
Bingham University, Nigeria
Email: **vonkera@gmail.com**

Abstract

In Nigeria today, most newsrooms are tightening their digital security due of concerns that new spy technologies have exposed journalists to threats of surveillance and digital harassment. The evolution of digital communication technology seems to have become a nightmare for most journalists within developed nations. These concerns affecting journalists seem to more often than not, originate from government coffers. This study aims to expose the intricacies surrounding the use of spyware technology to violate the professional and private lives of journalists in Nigeria and how the same hinders the free flow of information and press freedom. The research takes its theoretical leaning from the Communication Privacy Management Theory (CPM), a communication theory that focuses on why and how people manage private disclosures. The development of high-tech spyware poses a threat and is indeed an existential crisis for journalism and the future of press freedom around the world. The research recommends that the Nigerian National Assembly should urgently, initiate a legislation that guarantees the use of spyware technology in line with international human rights standards. Also, the national assembly should create legislation that ensures the federal government stops the abuse of "national security" to legitimize political surveillance. Journalists, especially, in Nigeria, should collectively upgrade–their digital devices by using State-of-The-Art software which encrypts their information in order to avert spyware attacks

Keywords: *Digital Security, Journalists, Press Freedom, Spyware, Surveillance*

Introduction

There is a growing list of safety risks within the digital domain, namely: journalists, internet shutdowns; surveillance; digital attacks and; inaccessibility to the technology that enables safe and secure communication. Journalism involves the handling and reporting of sensitive and important data that has a great risk of being stolen and mishandled. Walton (2023) posits that digital threats often come from countries that gather extensive information about journalists such as their whereabouts, networks, or sources. Authorities can use this intelligence to intimidate the media. This is why Maseko (2023) points out that in a digital world, attacks on journalists and journalism are not just limited to physical threats, with journalists increasingly receiving digital threats ranging from online harassment, digital monitoring, and hacking, and as a result, it has become important for journalists to be knowledgeable on digital safety. Abellan (2021) emphasized that cyber security and digital privacy are major concerns for today's journalists. With online threats becoming more prevalent and sophisticated, journalists today should understand how their data might be compromised, especially for investigative journalists. Data privacy and confidential data security should be essential elements of a journalist's job (Puredome, 2023).

In Nigeria, however, newsrooms are tightening their digital security measures out of concerns that new spy technologies have exposed journalists to even greater threats of surveillance and harassment. In his contribution, Yusuf (2023) states that the rapid expansion of the digital surveillance industry has enabled governments around the world to acquire new technologies to monitor journalists, silence independent journalism, and control the flow of information. The United Nations Human Rights (2022) exclaimed that digital surveillance of journalists is on the rise. They submit that the use of spyware has led to the arrest, intimidation and even killing of journalists. This trend is made manifest in the creation of fear in the minds of journalists thus silencing them in the long run. This surveillance syndrome entails an indignity to the professional and private lives of most journalists. The New York Times in 2021 reported that a coalition of news outlets accused an Israeli-based cyber surveillance company, NSO Group of supplying software that foreign governments use to surveil journalists (IAPP, 2023). The allegations focused on NSO's Pegasus, a surveillance application the coalition claims was used to attempt hacks on smartphones belonging to 37 journalists in several countries.

The use of spyware against journalist has become a growing concern, with many accusing governments and other powerful entities of using technology to surveil and intimidate journalists. Yusuf (2023) points out that concerns around digital technology and its role in democracy have been widely documented. He reiterates that since the emergence of social media platforms and the rise of digital communications, journalists, academics and, campaigners have been aware and vocal about the potential risks that these digital modes of communication expose us to. Walton, (2023) notes that the free speech rhetoric that often dominates contemporary discourse around social me dia and democracy ignores how dissenting voices become easy targets for wider suppression and surveillance, and that social media platforms are actively used for this purpose. To lend more credence to Walton's point, and online international daily, the Boycott, Divestment, Sanctions; BDS (2021) reported that in July 2021, Amnesty International in collaboration with tens of journalists and scholars exposed how the Israeli NSO Group's Pegasus spyware facilitated human rights violations around the world on a massive scale. Feldstein and Kot (2023) also assert that the global spyware and digital forensics industry continues to grow, despite public backlash following an array of surveillance scandals. This standpoint underscores the persistence of attacks on privacy and violation of the human rights of journalists especially in developing countries through spyware technology.

Nigeria as a developing nation is not excluded from this spy syndrome. Erezi (2021) contends that Nigerian states and the federal government have been using surveillance technologies to snoop on citizens' data and communications on their devices. Allegations of the Nigerian government spying on journalists is not new. He further notes that most states in Nigeria and the federal government hide under the guise of deploying technology to tackle societal challenges to reign in on private citizens, and journalists alike through snooping data and communication from their devices.

The research study aims to expose the intricacies surrounding the use of spyware technology to violate the professional and private lives of journalists in Nigeria and how the same hinders the free flow of information and press freedom.

Statement of the Problem

Violations of the freedom of speech and that of the press have taken a new dimension among developing nations like Nigeria (Marina, 2022). The evolution of digital communication technology seems to have become a nightmare to most journalists within these developed nations as these journalists are constantly at risk of being spied upon with state-of-the-art spyware without their knowledge and consent (Tsui and Lee, 2019). These espionage concerns by journalists seem to more often than not, originate from government coffers.

The use of spyware against journalists poses a serious threat to the profession, raising concerns about privacy violations. Munoz (2023) reports that there is a growing threat of spyware to journalism in Latin America, where reporters already face other forms of harassment and organized crime syndicates. Most governments in developing countries today have been alleged to constantly using spyware technology that violates the fundamental human rights of journalists by hacking into their digital devices in a bid to monitor their everyday activities and in the long run, use information from these digital spywares to silence journalists through various trumped-up charges and allegations. The study intends to proffer a solution to the above problem and elucidate on how spyware poses a threat to the professional activities of journalists.

Objectives of the Study

The study intended to achieve the following purposes at the end of the research:

1. Identify how the use of spyware technology impairs the professional ability of journalists to carry out free and fair reports devoid of digital impediments.
2. Elucidate on how spyware technology is used to identify, monitor and, silence journalists.
3. Elaborate the vulnerability of devices and digital accounts of journalists to surveillance technology.
4. Expatiate on the reluctance of credible sources of information to open up to journalists out of fear of being spied upon.
5. Expose the violation of freedom of information by spyware technology on journalists.

Conceptual Clarifications

Spyware

The first recorded use of the term spyware occurred on October 16, 1995, in a Usenet post that poked fun at Microsoft's business model. Spyware at first denoted software meant for espionage purposes. However, in early 2000, the founder of Zone Labs, Gregor Freund, used the term in a press release for the Zone Alarm Personal Firewall. Later in 2000, a parent using Zone Alarm was alerted to the fact that Reader Rabbit, an educational software marketed to children by the Mattel toy company, was surreptitiously sending data back to Mattel. Since then, spyware has taken its present sense (Sanklecha, Deotale, Yadav and Mishra, 2022).

Spyware is a malicious software that is designed to gather information about a person or organization without their knowledge or consent. It can infiltrate a computer or mobile device through various methods, such as downloading malicious software, clicking on infected links or attachments, or visiting compromised websites. Stafford and Urbaczewski (2018) contends that there are three major types of spyware which include: Adware: A spyware used to monitor a user's web browsing activity and send targeted advertisements to the user based on browsing activity. The second is named Keylogger: It's a spyware program designed to capture "log in" identity and password information finally, they talked about the Trojan Horses spyware, which is a spyware disguised as free software download. When installed, the Trojan Horses track and send information about the system to the author of the software.

Some of the known effects of spyware are consumption of system capacity, consumption of bandwidth, security issues arising from transmission of user information covertly and, privacy issues which border on invasion of privacy by spreading user information that may result in receipt of unsolicited commercial e-mails (Boldt, Carlsson and Jacobsson, 2020).

Once installed, spyware can track and record various activities, such as keystrokes, browsing history, login credentials, and even capture screenshots or record audio and video. It invades the device, steals sensitive information and internet usage data, and relays it to either advertisers, data firms or external users (Alexander, Brush and Teraveinen, 2021). Spyware is one of the most common threats to internet users. Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information. Patrick (2022) posits that spyware is a type of malware that tries to keep itself hidden while it secretly records information and tracks your online activities on your computers or mobile devices. It can monitor and copy everything you enter, upload, download and, store.

Furthermore, the state-of-the-art spyware used by experienced hackers today is called Pegasus. It has been described as a type of spyware that can infect mobile phones of targets through a variety of mechanisms. Some approaches may involve a message (SMS, iMessage, WhatsApp, email) that includes a link to a website. When clicked, this link delivers malicious software that infects a device (Kaldani and Prokopels, 2022). A more elaborate and clear explanation was by CISCO (2023) which submits that spyware is a malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. It is often used to steal financial or personal information from devices.

Digital Security

Digital security is the protection of digital devices and information from unauthorized access, use, theft, or damage. Digital security also encompasses the practices, strategies, and technologies employed to protect digital assets and systems from cyber threats, and malicious activities. Kumar, Gupta and Singh (2023) affirm that it involves the implementation of safeguards and measures to ensure confidentiality, integrity, and availability of information in digital formats. One of the components of digital security is encryption. This refers to the process of encoding information to make it unreadable to unauthorized individuals, ensuring that only authorized parties can access and understand the data. Authentication is another component of digital security which is the practice of verifying the identity of users, devices, or systems to ensure that only authorized entities are granted access to sensitive information or resources (Bellanova, 2023). The concept of digital security is critical in safeguarding personal information, commercial secrets, intellectual property, sensitive government data, and other digital assets from cyber threats, identity theft, data breaches, and cyber-attacks.

Digital security is becoming increasingly important in a world where we rely on digital devices and services to carry out important tasks such as banking, communication, and online shopping. Digital security includes various measures that are designed to ensure that data is safe from cybercriminals who may be attempting to steal it for malicious purposes in line with the assertions of Haunschild, and Bernhard (2023), Valistu (2023) and Hong and Zhang (2023). Ensuring digital security is important for both individuals and organizations. Digital security is crucial to keep sensitive information secure and maintain privacy, which is a fundamental right in today's digital age.

The 4th (Fourth) Estate

The Fourth Estate is a term used to refer to the press or news media as a valuable component of a functioning democracy. The term 'Fourth Estate' is believed to have originated during the French revolution, when the National Assembly was constructed with three estates, or orders of society - the clergy, the nobility, and the commoners (Mpofu, 2023). However, the press was seen as an important fourth power, essential to maintain transparency and hold those in power accountable. Today, the Fourth Estate refers to the role of the media in society. It is responsible for providing citizens with reliable information, investigative journalism, and analysis of important events and issues. Dewenter, Dulleck and Thomas (2020) aver that the Fourth Estate plays a critical role in holding government officials, elected representatives, and other powerful entities accountable for their actions. The Fourth Estate has been instrumental in shaping public opinion, promoting transparency, and exposing corruption and other abuses of power. However, the role of the Fourth Estate has also been criticized for its occasional bias and lack of objectivity.

In today's context, the Fourth Estate comprises journalists, news organizations, and media professionals who act as intermediaries between those in power and the public. They disseminate information, investigate and report issues of public interest, and act as conduit for public discourse and debate. Hansen (2018) succinctly notes that the Fourth Estate acts as a watchdog, monitoring the actions of government officials, exposing corruption or wrongdoing, and ensuring transparency in governance. Jensen (2020) emphasized that the concept of the Fourth Estate highlights the significance of a free and independent press in a democratic society, advocating for the freedom of the press, freedom of speech, and protection of journalists' rights. It emphasizes the responsibility of the media to inform the public, hold power accountable, and contribute to the functioning of a healthy democracy.

The Implementation and Practice of Freedom of Information ACT in Nigeria

Nigeria's Freedom of Information (FOI) Act was signed into law on May 28, 2011, after the longest legislative debate in the history of Nigeria. The debate lasted for over 12 years. The law was passed to enable the public access government information, in order to ensure transparency and accountability. The bill was developed by the Freedom of Information Coalition, a network of over 180 civil society organizations in Nigeria, comprising civil rights, grassroots and, community-based Non-Governmental Organizations campaigning for the Freedom of Information (FOI) Act to ensure accountability and transparency in public institutions in Nigeria. The FOI Act aims to make public records and information more freely available and to protect public records and information, in accordance with public interest and protection of personal privacy (Oluwasemilore, 2018).

In Nigeria, some of the failures and limitations of the Freedom of Information Act, according to Ogbuokiri (2021), is that it contains more exemption sections and clauses than sections that grant access to information. This means that some mischievous public officers can use these sections for unjust and mischievous purposes. For instance, Ogbuokiri submits that only Sections 1 and 3 grant access to information; but as many as ten sections (Sections 7, 11, 12, 14, 15, 16, 17, 18, 19 and, 26) are meant to deny the public access to information. However, the *omnibus* proviso against denial of information that says "where the interest of the public would be better served by having such record being made available, this exemption to disclosure shall not apply" is commendable, with the expectation that the Judiciary would interpret the proviso liberally for the public good. This shows that some of the exempted sections of the act could be used by the government to invade journalists' privacy and attack them via digital means, spyware included. According to Oberiri (2019) "there are always limitations as to what can be accessed in the operation of Freedom of Information, even in developed countries where the Freedom of Information Act has been in practice for long".

Freedom of information is an Act that was established in Nigeria on 28th May 2011 by an Act of the Federal Government of Nigeria to make public records and information more freely available, provide for public access to public records and information, protect public records and information to the extent consistent with the public interest and protection of personal privacy, and protect serving public officers from adverse consequences of disclosing certain kinds of official information without authorization and establish procedures for achievement of those purposes and for related matters (CBN, 2023). According to the United States Department of Justice (2023) the basic function of the Freedom of Information Act is to ensure informed citizens, vital to the functioning of a democratic society. Philip, Oluwaseyi and Emmanuel (2021) averred that more than a decade after the introduction of the Freedom of Information Act, most state governments in Nigeria have shown little or no desire to domesticate the legislation. They noted that only two states of Ekiti and Imo have passed a version of the Act within their states. Ezeh and Duru (2019) were also of the opinion that prior to the birth of the Freedom of Information Act, no law had guaranteed citizens access to public records and information.

Literature Review

The Proliferation of Spyware on Journalists' Activities

Some revelations regarding the apparent widespread use of spyware to attack journalists, human rights defenders, politicians and, others in a variety of countries are extremely alarming. This confirms the worst fears about potential misuse of surveillance technology to illegally undermine human rights. With regard to this, the United Nations Human Rights (2021) posits that companies involved in the development and distribution of surveillance technologies are responsible for avoiding harm to human rights. They need to take immediate steps to mitigate and remedy the harm caused by their products as well as carry out human rights due diligence to ensure that they no longer facilitate such undesired outcomes. In this vein, they avoid being involved in similar circumstances in the future. In a bid to buttress the standpoint of the United Nations Human Rights, Woodhams (2021) further asserts that the unchecked growth of the commercial spyware industry is providing repressive governments with new tools to surveil, harass and, attack independent journalists and their sources in a new battlefront against the free flow of information. His standpoint lends credence to the fact that most countries with a history of restricting free expression and weak legal and policy environments for safeguarding independent journalism could have a field day on their clamp-down against journalists who publish reports against their policies. Iroanusi (2021) was also of the view that activists, journalists, and politicians around the world have been spied on using cellphone spyware, igniting fears of widespread privacy and rights abuses.

The development of high-tech spyware poses a threat and existential crisis for journalism and the future of press freedom around the world. When spyware infects a phone, it can eavesdrop on a call before encryption takes place, much like "reading a letter over a writers' shoulder" before it is sealed in an envelope (Agence France Presse, 2022). The Committee to Protect Journalists (2022) contends that public reports of spyware attacks that undermine press freedom, particularly those involving products sold by private companies to state agencies is used to obstruct journalists and imperil their sources. The use of spyware against journalists is increasingly common, and not only among authoritarian governments in developing countries. Munoz (2023) reports that there is a growing threat of spyware to journalism in Latin America, where reporters already face other forms of harassment and organized crime syndicates. In particular, he emphasized that governments within the region are using this new weapon to discourage investigative reporting at a time of worsening corruption in the region. In a similar vein, the Nigerian government has invested heavily in the acquisition of surveillance equipment for its security agencies since at least 2014 and oftentimes, journalists are targeted with this technology. This stems from the fact that spyware software is marketed and licensed to governments around the world under the guise of protecting national security and public safety (Kabir and Adebajo, 2023).

Spyware Technology and its Impediment on Journalism

Nigerian journalists are increasingly under threat from digital and physical surveillance. This reinforces the value of internet-based, encrypted communications at a time when authorities have also targeted journalists' phones and computers to reveal their sources. Yusuf (2023) notes that newsrooms are tightening measure at digital security due to concerns that new spy technologies have exposed journalists to even greater threats of surveillance and harassment. Azu (2022) points out that a good number of journalists had become victims of surveillance, spying, harassment, threats, violence, assaults and, arbitrary arrests, among others. Haddad (2022) also emphasized that spyware technology poses an existential challenge for journalism. This insidious technology compromises editorial planning and can dissuade journalists from reporting on critical stories or discourage would-be sources from coming forward, carving a hole into the very fabric of journalism. Onuche (2022) further asserts that spyware espionage on journalists in Nigeria could take the form of attacks: denial of service; distributed denial of service; cyber-stalking, man-in-the-middle; social engineering/phishing; and; disinformation or mal-information.

Spyware enables governments, entities, or individuals to monitor and track journalists' activities, including their communications, online behavior and physical location. Silic (2022) reports that in December 2020, twenty-five (25) governments had acquired surveillance systems from *Circles*, a company that produces spyware equipment. These countries are: Australia, Nigeria, Belgium, Botswana, Chile, Denmark, Equatorial Guinea, Ecuador, El Salvador, Estonia, Guatemala, Honduras, Indonesia, Israel, Kenya, Malaysia, Mexico, Morocco, Peru, Serbia, Thailand, the United Arab Emirates, Vietnam, Zambia and Zimbabwe. This report adds to a growing public record of misuse of spyware equipment globally, especially against journalists. Another investigation by Anyaogu (2022) shows that when anything is published online, there are some hired people by government officials to track the source of the publication and create means to hack the device used to publish the information without the author's knowledge. To this end, surveillance can expose information gathered by journalists, including whistle blowers, and violate the principle of source protection, which is universally considered a prerequisite for freedom of the media and freedom of information.

Use of Spyware and its implication on Journalist's Freedom and Safety in a Digital Era

Spyware allows for invasive surveillance of journalists' digital activities, including monitoring their communications, browsing history, and personal information. Okocha, Chigbo and Onube (2022) assert that the increasing trend in digital authoritarianism across the world with media personnel bearing the brunt is largely due to the state's determination to control information dissemination in the digital age. There is nothing new about governments spying on journalists or activists they fear might expose or discredit them. But the development of high-tech spyware-the kind that takes over a phone without a user's knowledge or interaction, poses an existential crisis for journalism and the future of press freedom around the world. Mraadmin (2021) reports that the negative impact of commercial spyware on journalist's safety is unmistakable, especially when the information that the spyware extracts promote physical attack, or even the murder of journalists or news sources. This demonstrates that impact of spyware on journalists globally. However, this extends far beyond the journalists and sources directly targeted. The Media Development Investment Fund (2022) reported that at times of conflict and disruption to mainstream channels, the media and journalists alike need to engage with audiences on social media more than ever, not only to share information but also to provide a platform for debate. However, increased activity can attract the unwelcome attention of hostile digital forces that stall journalist's reports via digital espionage. If this activity is not curtailed, it can immensely stifle journalist's activities.

To shed more light on the discourse, Mills (2019) posits that surveillance has been indicated as having a potential chilling effect on journalism and as a phenomenon fueling fear and paranoia among journalists. This has led to many journalists altering their behavior and turning down sensitive stories that can contribute to societal awareness and development when disseminated. Consequently, a growing body of findings and resolutions both at the universal and regional levels, suggests that international disruptions of the internet, violate international law. In 2015, in a joint declaration on freedom of expression and conflict situations, the UN and regional monitors of freedom of expression declared that the filtering of content on the internet, using communications "kill switches" (shutting down entire parts of communications systems) are measures which can never be justified under human rights law (Gowacka, Youngs, Pintea, and Wolosik, 2021).

Journalists in Nigeria today are navigating "treacherous waters" more than any time in recent memory. Despite a plethora of digital tools to keep them safe, many journalists fail to adopt to new strategies. Woodman (2018) proffered some safety security tips that most journalists ignore even though it exposes them to safety and surveillance risk in the digital environment. He mentioned the failed use of end-to-end encrypted applications which ensure encryption of calls and messages, insecure encrypted digital file storage, use of easy to decipher passwords, and failure to deploy two factor authentication on digital platforms. Tsui and Lee (2019) aver that if journalists make the best use of holding powerful institutional actors accountable; then, they need to be free from the surveillance by these powerful institutional actors. They stressed the need for compliance with security protocols by journalists when uploading information on digital platforms. This strategy enhances the safety of information sources.

Information security is becoming increasingly essential for journalists around the world. While most will probably not be targeted by spyware, all journalists face a threat of some level from a variety of possible attacks. Henrichsen (2019) was of the view that a significant number of journalists do not believe that hacking and surveillance are significant threats, and they are not adopting information security measures to protect their data, themselves or their sources. He further notes that when journalists' digital accounts are vulnerable to hacks or surveillance, news organizations, journalists and their sources are at risk; and the journalists' ability to carry out their news gathering and dissemination functions are reduced. Marina (2022) suggests that journalists should take some time to evaluate their digital security by using encryption tools, use of multiple devices and not to dwell on the assumption that you will not be targeted as a journalist. Lewis (2020) adds that for efficient digital security, journalists should avoid reused passwords and PINs across devices, and all data should not be treated the same by journalists. Digital security and safety is an issue for every practicing journalist today. Digital infrastructure has become a critical part in the functioning of society today and improving the quality of life in this fast-paced world of ours today.

Spyware and Violation of Human Rights on Free

Expression and Privacy in the Digital Age

In the modern world, almost every act online is an act of expression (Adenle, 2022). These online acts include: chatting online; networking with friends and colleagues, surfing websites, reading news; and downloading files etc. These are all acts of imparting or accessing information. In online interactivity, there is content generated and stored, some of which is publicly available, most of which is amongst select individuals and groups. Yet each of these acts also generates information Internet from the various transactions that occur and can be monitored by unintended parties. In turn, nearly every act of expression is now observable to communications providers. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) protects everyone from arbitrary or unlawful interference and violation of privacy, family, home or correspondence. The international human rights community has begun the process of responding to the erosion of privacy rights that new technologies have facilitated. This report recommends that the U.N. Human Rights Committee assist in this process by issuing a new General Comment on the right to privacy under Article 17 of the ICCPR (American Civil Liberties Union, 2023).

The constitution of Nigeria provides for the freedom of information in section 39 of the 1999 constitution as amended in 2018. In furtherance to this, the country had constituted a Freedom of Information Act in 2011 as a legal document to provide a leeway for journalists and other media practitioners alike to access information to aid their professional assignment without let or hindrance. The Act was signed into law on May 28 2011, after the longest legislative debate in the history of Nigeria. The debate lasted for over 12 years (Oluwasemilore, 2018). It is however sad to note that more than a decade after the Act was passed into law in the country, no fewer than 16 states have yet to domesticate it or create comparative and parallel mechanisms that serve to promote transparency and accountability in government. The 16 states include Imo, Anambra, AkwaIbom, Edo, Osun, Ogun, Plateau, Kogi, Nasarawa, Niger, Kano, Sokoto, Bauchi, Adamawa, Taraba and Yobe (Okereke, 2020). It is important to note that accessing records has become a herculean task for most journalists in Nigeria today. Ndidiamaka, Awo and Obiageri (2021) posit that the time it takes to access official records in Nigeria today is rather too long especially in the world today where information moves at the speed of light. Adenle (2022) further submits that the government in Nigeria today feels that it is legal to restrain the power of the press and if possible, have total control of the press. To the Nigerian government, the press is an instrument of people in power; so, it should yield itself to their dictates. The Freedom of Information Act should serve to embolden the media to provide models for the flourishing of open governance, gender-balancing and, unencumbered access to government affairs, not merely records and documents which are saddled with official cover-ups or distortion (Omoera, 2021).

The use of spyware often involves disproportionate interference with individuals' rights. It intrudes upon their private spaces and communications without warrant or legitimate justification. Samuel (2019) asserts that the essence of journalism which is to provide citizens with reliable information through discipline of verifications; such information cannot be available without unhindered access to information, which some scholars argue that it plays a key role in a system of checks and balances. Chukwu (2019) emphasizes this standpoint when he contends that the journalists' first loyalty should be to the citizenry; they are obligated to tell the truth and must serve as an independent monitor of powerful individuals and institutions within the society. Opeyemi (2022) notes that more often than not, journalists in Nigeria face different forms of harassment for coverage and or publishing information that are perceived to be offensive to the government or their agents. Meanwhile, Todah (2022) was also of the view that the distinction in press freedom during the military-era versus in our current democratic leadership is hazy- particularly since around the world, the press is facing new challenges such as navigating digital surveillance, hacking, online harassment and internet shutdowns. Samuel (2019) also pointed out a situation where all relevant documents that will aid the successful operation of journalists are classified as "Allied matters", which is official secret, leaves nothing to be desired of Nigeria. This situation as pointed out by him denotes that journalists in Nigeria today are limited in their professional practice due to a conflicting interest of the freedom of information act and the official secrets act. In this light, Njoku (2019) pointed out that journalists must know that freedom must be matched with responsibility. Njoku (2019) contends that although the freedom of information act contains more exemptions sections and clauses than sections that grant access to information, journalist should not relent in the discharge of their duties to the society.

Selected Cases of Use of Spyware against Journalist in Nigeria

Spyware compromises the anonymity and safety of sources, making it easier for authorities or other malicious actors to identify and retaliate against them. Ajaikaiye (2022) reports that in 2018, Azeezat Adedigba, a reporter at the time with *Premium Times*, a digital news platform was about her duties when she received a call from an unfamiliar line. She didn't pay attention until the calls became incessant. The call would later turn out to be an invitation from a police officer who tracked her movement through her mobile device. She was subsequently summoned to appear at the police headquarters Abuja over one Ogundipe, a colleague of hers, who was later arrested for refusing to disclose the source of a story involving a former Inspector General of Police, Ibrahim Idris. As colleagues working for one of Nigeria's reputable digital publishing platforms, both reporters often spoke over the phone about their work, unaware that their regular conversations were being monitored by security personnel.

In another development, the Committee to Protect Journalists (CPJ) reported that the State Security Service (SSS) swooped on *Daily Trust* newspaper offices in Maiduguri and Abuja in October 2021, detaining two of its staff, Ibrahim Sawab and Uthman Abubakar. According to the security personnel, the newspaper had divulged classified information undermining national security and contravening Nigeria's Official Secrets Act for its report on the Nigerian military effort to retake six towns from Boko Haram. They were able to establish the reason for the raid through active digital surveillance of the media house through spyware technology. The report by the Committee to Protect Journalists stated that a total of 376 attacks on journalists in Nigeria have been documented. Of this, 373 reports have been verified and 198 violent cases reported (Centre for

Journalism, Innovation and Development, 2021).

By monitoring journalists' communications and activities, spyware enables intimidation and threats against them. Knowing they are being surveyed, journalists may face increased pressure, harassment, or physical harm. Yusuf (2023) notes that in 2019, two Nigerian journalists, Gidado Yushau and Alfred Olufemi were charged with criminal conspiracy after the Nigerian police tracked their phones and alleged that they published malicious materials online. They are still facing trial in Ilorin, Kwara State. Yusuf further points out that the Nigerian military is using surveillance technology to spy on ordinary Nigerians and the press. He stated that the Nigerian military targeted journalists' phones and computers with forensic equipment procured from an Israeli-based company to monitor and interrogate journalists. Some experts believe that when the devices of journalist and their sources are vulnerable to surveillance, the ability of journalists to carry out their news-gathering function is significantly diminished.

Investigative journalism relies on rigorous research and protection of sources. The use of spyware undermines these essential practices and obstructs journalists' ability to deliver in-depth, unbiased reporting. Telloglou (2022) reported that a journalist, Ogunmola Segun, who works for an international investigative platform known as *ANT1 news* confirmed the hacking of his phone through the use of a predator spyware by an unknown party whom he believed had put him under surveillance for publishing an article on a spyware scandal. In another development, a journalist, Tanimola Peters, a correspondent for BBC (*British Broadcasting Corporation*) in Nigeria, revealed that a publication he made on the alleged corruption in the office of the Attorney General of Nigeria's office made his story to be disparaged and attacked by counter story-tellers. An investigation by an international agency known as *Citizen Lab and Access* had confirmed that these alleged 'story-tellers' was actually Pegasus spyware that hacked his system (Dan and Aranda, 2023).

In another matter, Komlanvi Ketohou, a Togolese journalist working in Nigeria for an online newspaper in Lagos, fled to the United Kingdom in early 2021, he left behind his home, his family, and his cell phone that was seized by the Nigerian State Security Service (SSS) when they arrested and detained him over a report published by the online newspaper he was working for. In July of the same year, he learned that the phone number connected to his phone that the security personnel took may have been targeted for surveillance, years before his arrest. The revelation came via the Pegasus project, a collaborative global media investigation detailing how thousands of leaked phone numbers, including many that belonged to journalists, were allegedly selected for potential surveillance by clients of the Israeli firm, NSO Group (Committee to Protect Journalists, 2022). In addition, Dan and Aranda, (2023) also reported that on 15th April, 2020, Michael Ikeogwu, and Matthew Omonigho of the *Daily Post* newspaper were assaulted by men from the State Security Service (SSS) for a report that was traced and alleged to have emanated from the email of Michael Ikeogwu during the lock-down period accompanying the COVID 19 surge.

Mitigating against Spyware and Security Breach

Mitigating against spyware and security breaches requires a multi-faceted approach that involves both preventive and responsive measures. Tom and Akpan (2022) proffered the following to mitigate against spyware and security breaches. First, they talked about the use of firewalls, which is a software device that blocks certain network traffic, use of Software solutions which exists to identify and remove malware and to help manage spam email; the use of authentication, which involves determining that a particular user is authorized to use a particular computer. They also talked about hardware cryptography, which entails the use of computer chips with cryptographic capabilities intended to protect against a range of security threats. Finally, they mentioned the use of patches which are programs designed by software manufacturers to fix software security flaws. Cheng, Liu and Yao (2018) also contributed on this factor when they stated that the use of privacy preserving data leak detection, which is a software that utilizes the MapReduce distributed computing framework to inspect sensitive content for inadvertent data leak detection, can be deployed either in local computer clusters or in the cloud.

Another view was that the prevention of spyware attachments could be mitigated through a prevention mechanism to protect against a spyware known as keylogger attack. This is done in three phases which include, the use of a device known as honey pot which is a software installed in an individual's system to monitor malicious activities and remove same by the help of a prevention server (Wazid, 2020). Agrawal, Varshney, Kakandwar and Singh (2022) also submit that journalists should avoid clicking on any link on the internet, if they are not from a trusted source. Also journalists should ensure that they update their software with official patches released by trusted organizations and that avoidance of public networks should be strictly adhered to. Manasah and Devi (2023) also noted that the use of strong passwords, changing of passwords frequently and checking of emails thoroughly could serve to mitigate against an influx of spyware in computer and phone components.

Internet surveillance has become a crucial issue for journalism. Many journalists and their sources, over the years, face different kinds of risk while communicating online. Salvo (2021) observed that due to the sensitivity of the work of most journalists, investigative reporters in particular, have been placed in dangerous positions when the need arises for potential chilling effects of surveillance on their work. Wu, Wang, Kua and Huang (2018) recommend the use of a software known as STARS (Stateful Threat-Aware Removal system) for journalists. This is a software tool that studies system behavior, and ensures that removed spyware programs do not reinstall themselves, to enforce information flow policy in the journalists system. To ensure the protection of journalist's sources of information, Saxena (2020) avers that journalist should ensure that messages from sources are properly encrypted using the plethora of encryption applications available from software companies to safeguard back and forth information from both parties from the risk of surveillance. This method could prove to be highly effective if most journalists, especially the investigative journalists are aware of these encryption software and use. them

Theoretical Foundation

The research takes theoretical leaning from the Communication Privacy Management Theory (CPM). It is a communication theory that focuses on the idea of why and how people manage private disclosures. The theory was created by Sandra Petronio in 1991 (Petronio, 2020). The theory focuses on the importance and maintenance of privacy and how it is navigated in the scope of communication. Self-disclosure and the management of private information can change based on different personal experiences (Nodulman, 2021). While some people are comfortable sharing all information with their significant other, some may not share more personal details about their lives. The theory hinges upon the idea of weighing and comparing pros and cons in order to decide courses of action in communication when considering privacy boundaries. It posits that self-disclosure is an ongoing dynamic process with communicators making daily decisions of what to disclose to others.

Some of the assumptions of the theory is that humans are choice makers, humans are rule makers and rule followers, human choices and rules are based on a consideration of others as well as self, relational life is characterized by change, and that contradiction is the fundamental fact of relational life. Some basic suppositions of the theory postulates that private information, which borders on aspects which matter deeply to a person namely: private disclosure, which hinge on the process of communicating private information to another, and private boundaries, which provide for the demarcation between private information and public information (Dindia, 2020).

The basic criticism of the theory was that it uses the term dialectic inaccurately. The theory is premised on the Socio-cultural tradition of communication from an interpersonal communication context with an interpretative approach to knowing.

The theory is relevant to the study because information contained on digital devices is personal to the owner of the same. Thus, disclosure of such information should be done with mutual consent devoid of privacy violation.

Methodology

The research work relies on the descriptive method of research. Information is therefore sourced from books, journals, periodicals, newspapers, magazines, government publications and, online sources. Descriptive research is a research method that describes the characteristics of the population or phenomenon that is being studied. This methodology focuses more on the "what" of the research subject rather than the "why" of the research subject. In other words, descriptive research primarily focuses on describing the nature of a demographic segment without focusing on why a certain phenomenon occurs (Sri, 2019).

Conclusion

Use of spyware as a weapon of unwarranted espionage on journalists across the world including Nigeria goes unabated. Journalists especially in Nigeria today are compelled to constantly look out for the security of their digital gadgets for fear of intrusion from unknown sources that are always on the prowl for information from such journalist's devices. This fear has permeated to information sources. Through knowledge of how journalists' devices are being preyed upon, they advise extreme caution in revealing information that advances the cause of investigative reports as these are usually for public consumption. As advancement in communication technology soars, espionage technology via spyware appears to be at par with this perceived advancement. This calls for more safety precautionary measures by journalists and their information sources alike. They must beware of privacy violations perpetrated by spyware.

Recommendations

The study made the following recommendations:

1. The Nigerian National Assembly should as a matter of urgency, initiate a legislation that will guarantee the use of spyware technology in line with international human rights standards.
2. The National Assembly should also create a legislation that ensures the Federal Government of Nigeria stops the abuse of national security purposes to legitimize political surveillance.
3. Journalists, especially in Nigeria, need to properly educate themselves through workshops, seminars and conferences on digital safety adherence. This will safeguard their information from spyware attacks.
4. Journalists especially in Nigeria should collectively see to the upgrading of their digital devices by using state of the art software that encrypts their information in order to lessen the impact of spyware attacks.
5. The Nigeria Union of Journalists (NUJ) should be more proactive in the enforcement of the laws against disclosure of information sources to avoid unnecessary human rights violations by Nigeria's security personnel.

References

Abellan, A. (2021). Privacy day 2021: what journalist need to know. *A digital security guide to staying safe online.* www.datajournalism.com/read/longreads/privacy-day-security-guide retrieved on 17/03/2023

Agrawal, M., Varshney, G., Kakandwar, S., Singh, K.P. (2022). Pegasus: zero-click spyware attack-its countermeasures and challenges. *Regional journal of information science* 5 (1). www.doi.org:10.13140/RG.2.2.21979.90405 retrieved on 15/03/2023

American Civil Liberties Union (2023). The human right to privacy in the digital age. www.aclu.org/other/human-right-privacy-digital-age retrieved on 18/04/2023

Adenle, Y. I. (2022) Impact of freedom of information act on journalism practice in Nigeria. *Online journal of communication and media technologies,* 4 (1). www.ojcmt.net retrieved on 15/03/2023

Agence France Presse (2022, October 13) Spyware poses dire threat to journalists, media watchdogs.www.voanews.com/amp/spyware retrieved on 15/03/2023

Ajaikaiye, H. (2022). How Nigeria's state surveillance crackdown on journalists, active citizens. www.africachinareporting.com/data-trails-how-nigerias-state-surveilance-crackdown-on-journalists-active-citizens/

retrieved on 12/03/2023

Alexander, S.G, Brush K, & Teranvainen, T. (2021). Spyware: threats and vulnerabilities.www.techtarget.com retrieved on 17/04/2023

Anyaogu, I. (2022, May 03). World press freedom: Nigerian media under digital siege.www.businessday.ng retrieved on 18/04/2023

Azu, C. J. (2023, April 04). World press freedom day: Nigerian journalist decry worsening conditions. www.dailytrust.com/world-press-freedom-day retrieved on 12/03/2023

BDS (2021). Israeli spyware facilitates human rights violations. www.bdsmovement.net/israeli-spyware-facilitates-human-rights-violations retrieved on 15/04/2023

Bellanova, R. (2023). Digital security and violence. *Security studies. Critical perspectives* 239-255. Oxford university press.

Boldt, M., Carlsson, B., & Jacobsson, A. (2020). Exploring spyware effects. *International journal of intelligence and counterintelligence*. www.doi.org.10.1109.2020.382 retrieved 12/03/2023

CBN (2023) Freedom of Information Act: The freedom of information act and war against transparency. www.cbn.gov.ng retrieved 14/03/2023

Cheng, L., Liu, F., Yao, D.D. (2018). Enterprise data breach: cause, challenges, prevention and future directions. *Wiley journal of inter-disciplinary reviews* 7 (3). www.doi.org:10.1002/widm.1211 retrieved on 15/03/2023

Chukwu, J.O. (2019). The challenges of implementing the freedom of information act by journalist in Lagos state, Nigeria. *Journal of management sciences*, 13 (1). www.doi.org:10.26524.jms.13.12 retrieved on 10/03/2023

Cisco (2023). What is malware? www.cisco.com/site/us/en retrieved on 13/03/2023

Centre for Journalism Innovation Development.(2021). Nigerian military using surveillance technology to spy on Nigerians. www.thecjid.or/nigerian-military-using-surveillance-technology-to-spy-on-nigerians-cpj/ retrieved on 15/03/2023

Committee to Protect Journalist (2022). Spyware and press freedom. *When spyware turns phones into weapons*. https://www.cpj.org/spyware retrieved on 18/04/2023

Dan, S. &Aranda, T. (2023). The risks commercial spyware poses to journalists, activists and government officials. www.pbs.or/newshour/show/ retrieved on 17/03/2023

Dewenter, R., Dulleck, W. & Thomas, T. (2020). Does the 4th estate deliver? The political coverage index and its application to media capture. *Journal on constitutional political economy* 31 (3): 8-14. www.doi.org/10.1007/s10602-019-5 retrieved on 19/10/2023

Dindia, K. (2020). The relationship. In theories of human communication. Wadsworth publishers.

Ezeh, N. &Duru, C.W. (2018). Nigeria's freedom of information act: opportunities and challenges. *Global journal of applied management and social science*, 15 (3), 51-58. ISSN:2276-9013.www.gojamss.net retrieved on 04/04/2023

Erezi, D. (2021). New report claims Nigeria is spying on its citizens' data and communications.www.guradian.ng/news/new-report-claims-nigeria-si-spying-on-its-citizens-data-and-communications/ retrieved on 17/03/2023

Feldstein, S. &Kot, B. (2023). Why does the global spyware industry continue to thrive? Trends, explanations, and responses.www.carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229 retrieved on 18/04/2023

Glowacka, D, Youngs, R, Pintea, A &Wolosik, E (2021). Digital technologies as a means of repression and social control.www.europa.cu/RegData/etudes/STUD/2021/653636/EXPO_STU(2021) retrieved on 14/03/2023

Haddad, W. (2022). Spyware poses an existential crisis for journalism and threatens press freedom around the world. retrieved on 18/04/2023

Hansen, E. (2018). The fourth estate: the construction and place of silence in the public sphere. *Journal of philosophy and social criticism*, 44 (1): 19-25. www.doi.org/10.1177/01914537187979991 retrieved on 19/10/2023

Haunschild, I. & Bernhard, L. (2023). The use of digital media and security precautions in adulthood. Journal of human behavior and emerging technologies 13 (4): 1-9. Retrieved on 19/10/2023

Henrichsen, J.R. (2019). Breaking through the ambivalence: journalistic responses to information security technologies. *Journal on digital journalism.* 8 (3). Pp 19-20. www.doi.org:10.1080/2160811.2019.1653207 retrieved on 17/04/2023

Hung, W. & Zhang, W. (2023). Digital identity, privacy, security and their legal safeguards in the metaverse. *Journal of security and safety* 2 (5): 4-6. www.doi.org/10.105/sands/2023011 retrieved on 19/10/2023

International Association of Privacy Professionals (2023). Surveillance abuses via spyware.www.iapp.or/news/a/journalist-allege-surveillance-abuses-via-spyware/ retrieved on 17/03/2023

Iroanusi, Q.E. (2021). Private Israeli malware used to spy on journalist, activist and politicians.www.premiumtimesng.com retrieved on 19/03/2023

Jensen, E. A. (202). Between credulity and sceptism: envisaging the fourth estate in 21st century science journalism. *Journal on media culture and society* 32 (4): 615-630. www.doi.org/10.1177/0163443710367695 retrieved on 19/10/2023

Kabir, A & Adebajo, K. (2023). How digital surveillance threatens press freedom in West Africa. www.humananglemedia.com retrieved on 12/04/2023

Kaldani, T & Prokopels, Z. (2022). Pegasus spyware and its impacts on human rights. www.rm.coe.int/pegasus-s retrieved on 10/04/2023

Kumar, S., Gupta, U & Singh, A.K. (2023). Artificial intelligence: revolutionizing cyber security in the digital era. *Journal of computers mechanical and management.* www.doi.org/10.57159/gadl.jcmm.2.3 retrieved on 19/10/2023

Lewis, K.P. (2020). Digital security do's and don'ts for journalists. *Digital and physical safety*.www.ijnet.org/en/story/digital-security-dos-and-donts-journalists retrieved on 10/04/2023

Manasa, R. & Devi, J.A. (2023). Cyber security attacks detecting thread in the virtual world of corporate sectors. *International journal of case studies in business, IT and education.* 7(2). www.doi.org:10.47992/IJSBE.2581.6942.0261 retrieved on 18/04/2023

Marina, A. (2022). Why journalism needs information security: risks facing journalist and how they can protect themselves.www.reutersinstitute.politics.ox.ac.uk/caledar/why-journalism-needs-information-security retrieved on 09/03/2023

Maseko, L. (2023, Feb 9). How to protect yourself online as a journalist. www.jamlab.africa/how-to-protect-yourself-online-as-a-journalist/ retrieved on 12/04/2023

Media Development Investment Fund (2022). Digital attacks are becoming weapon of choice to silence media.www.mdif.org/digital-attacks-silence-media/ retrieved on 10/03/2023

Mills, A. (2019). Now you see me-now you don't: journalist's experiences with surveillance. *Journal on practice of journalism.* 13 (6), 690-701. www.doi.org:10.1080/08900/0520701315806 retrieved on 20/04/2023

Mpofu, S. (2023). Monitoring the fourth estate: a critical analysis of the role of audiences in watchdogging journalists. *New journalism ecologies in east and southern Africa*, 183-205. www.doi.org/10.1007/978-3-03-23625-9_11 retrieved on 19/10/2023

Munoz, B. (2023). Journalism in Latin America is under attack by spyware. www.wilsoncenter.org/blog-post retrieved on 11/03/2023

Mraadmin, S. (2021 September 06). Report on use of spyware to silence journalists.www.mediarightsagenda.org/cima-releases-new-report-on-use-of-spyware-to-silence-journalist/ retrieved on 13/04/2023

Ndidiamaka, F.A., Awo, N.M., &Obiageri, O.A. (2021). Freedom of information act and journalism in Nigeria, 2011-2021: a review of a decade of utilization and practice. *The melting pot journal*. 6 (1).www.aphriapub.com/index.php/TMP/article/view/1381 retrieved on 10/03/2023

Njoku, C. (2020). Investigative journalism and freedom of information act in Nigeria. retrieved on 9/04/2023

Nodulman, J.A. (2021). *Self-disclosure, identity and relationship development*: a dialectical perspective. John Wiley & Sons Ltd.

Oberiri, D.C. (2019). An appraisal of the freedom of information act (FOIA) in Nigeria. *Canadian Journal of Social Science* 3 (3). www.doi.org.10.53103/cjss retrieved on 11/03/2023

Ogbuokiri, K. (2021). Nigeria: the limit of information act in freedom of information act 2011 and the fight against corruption and corporate fraud in governance.www.allafrica.com retrieved on 13/04/2023

Okereke, I. (2020, August 14). How state officials violate Nigeria's freedom of information act. www.premiumtimesng.com retrieved on 14/04/2023

Okocha, D.O., Chigbo, M. &Onube, M.J. (2022). Digital authoritarianism in Nigeria: *internet control techniques and censorship. Journal of community & communication research.* 7(1). www.jccr.sccdr.org retrieved on 13/04/2023

Oluwasemilore, I (2018) A critical Analysis of Nigeria's freedom of Information Act. *The Gravita's Review of Business and Property Law* 9 (2).www.gravitasreview.com.ng retrieved on 19/03/2023

Onuche, P. (2022). Spyware poses an existential crisis for journalism.www.cpj.org/newreport retrieved on 18/04/2023

Omoera, O.S. (2021). The quest for more effective media and the freedom of information act in *Nigeria.Sinestesienoline journal* 12 (5). ISSN: 2280-6849. www.sinestesieonline.org retrieved on 10/03/2023

Opeyemi, A. I. (2022). Democracy and stiffened media freedom in Nigeria: the seemingly unbridgeable gap. www.fesmedia-africa.fes.de retrieved on 10/03/2023

Patrick, S. (2022). What is spyware? Who can be attacked, and how to prevent it.www.avast.com/c-spyware retrieved on 15/03/2023

Petronio, S. (2020). Boundaries of privacy. *Dialectics of disclosure*. SUNNY Press.

Philip, T.D., Oluwaseyi, S., & Emmanuel S. (2021). 10 years of freedom of information act in Nigeria. The journey so far. Prospects and Challenges among media practitioners. International journal of social relevance & concern 9 (8). www.doi.org:26821/JSRC.9.8.2021.9841 retrieved on 14/03/2023

Puredome (march, 19 2023). VPN for journalist and bloggers. www.puredome.com retrieved on 19/03/2023

Salvo, D.P. (2021). Investigative journalists and internet surveillance. *International journal on journalism practice*, 16 (4). www.doi.org:10.1080/17512786.2021.201436 retrieved on 18/04/2023

Samuel, N. (2019). Press freedom in Nigeria legal bases and constraints. *Journal of current issues in arts and humanities*. 5 (1). www.idosr.org retrieved on 15/04/2023

Sanklecha, S, Deotale, D., Yadav, B.J., & Mishra, D.M (2022). Spyware. *International journal of research in applied science*. www.doi.org.10.22214/ijraset.2022.42200 retrieved on 17/04/2023

Saxena, J. (2020). A holistic approach to data protection for journalists. *International journal on computers and information technology*. 10 (3) www.doi.org:10.1393/8744/65948721.2020.202497 retrieved on 04/05/2023

Silic, A. (2022). The use of spyware against dozens of activist women in the middle-east.www.theintercept.com/2022 retrieved on 15/03/2023

Sri, S. (2019). Descriptive research. Journal of economics and technology research.www.jetr.org/papers/JETR/190597.pdfretrieved on 18/04/2023

Stafford, T, &Urbaczweski, A. (2018). Spyware: the ghost in the machine. *Journal of communications of the Association for information systems*. www.doi.org.10.56553/cais-2018.0013 retrieved on 04/04/2023

Tellglou, T. (2022). Revelations of spying on journalist. International press institute. www.ipi.media/ retrieved on 4/05/2023

Todah, O. (2022). The reality of press freedom in Nigeria. What are journalists saying? retrieved on 15/04/2023

Tom, J.T., &Akpan, A.G. (2022). Cyberspace: mitigating against cyber security threats and attacks. *International journal of engineering and technical research* 11(1). www.ijert.org retrieved on 15/04/2023

Tsui, L and Lee, F. (2019). How journalist understand the threats and opportunities of new technologies: a study of security mind-sets and its implications for press freedom. *Sage journals.* 22 (6). www.doi.org/10.1177/1464884919849418 retrieved on 18/04/2023

United Nations Human Rights (2022). Use of spyware to survey journalist and human rights defenders. www.ohchr.org/en/2021/07 retrieved on 17/03/2023

United States Department of Justice (2023). Freedom of information act and government. www.foia.gov retrieved on 18/04/2023

Vallistu, J. (2023). Digital social security accounts for platform workers. *International Journal of social security* review 16 (3): 3-4. www.doi.org/10.1111/issr.1237 retrieved on 19/10/2023

Walton, A. (2023). If journalist aren't protected, free speech means nothing. www.newarab.com/opinion/if-journalist-arent-protected-free-speech-means-nothing retrieved on 12/03/2023

Wazid, M. (2020). Implementation and Embelishment of prevention of keylogger spyware attacks. *Springer journal of computer and information science*, 13 (7). www.doi.org:10.1007/978-3-642/40576/1/26. Retrieved on 18/04/2023

Woodhams, S. (2021). Spyware: an unregulated and escalating threat to independent media. www.cima.ned.org/publication retrieved on 20/03/2023

Woodman, C. (2018). Digital security tools for protection of work and sources for journalists. www.icij.org/inside-icij/2018/01 retrieved on 13/04/2023

Wu, M.W, Wang, Y.M, Kuo, S.Y & Huang, Y. (2018). Self-healing spyware: Detection, and remediation. *IEEE journal on transactions and reliability*, 56 (4). www.doi.org:10.1109/TR.2007.909755 retrieved on 18/03/2023

Yusuf, K. (2023). Heightened surveillance by security operatives puts Nigerian journalist under climate of fear. retrieved on 02/04/2023