LEAD CITY INTERNATIONAL JOURNAL OF LIBRARY, INFORMATION & COMMUNICATION SCIENCES
[LCIJLICS]. ISSN: 3027-0022, eISSN: 3027-0901
VOL 2. ISSUE 2. JULY 2025 (DOI: https://doi.org/10.63741/lcijlics.2025.0202.03-j)

DIGITAL FOOTPRINT IN JOURNALISM: COVERING THE TRACKS BY THREAT-PRONE JOURNALISTS IN NIGERIA

Bayo I. Oloyede & *Mayokun J. Owojuyigbe
Redeemer's University Department of Mass Communication
P.M.B 230, Ede, Osun State, Nigeria

Email address of *corresponding author:
owojuyigbem@run.edu.ng

ABSTRACT

This paper examined the unique security challenges posed by digital media use among Nigerian journalists, and the remedies that help mitigate the fast-growing threats. The study employed exploratory research design, while using literature review as a research instrument. Analysis of secondary data gathered from reviewed literature, Internet resources, and library materials, form the basis for discussion of digital journalism practice in Nigeria, its pros and the subtleties of digital security challenges that largely constitute its cons. Digital security trends in Africa were examined, vis-à-vis the lag in preparedness of African nations, including Nigeria, to tackle these security concerns at a level similar to efforts in developed countries. Technology Acceptance Model (TAM) formed the theoretical framework for this study, with its Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) components. A third component, 'Perceived Threat of Use' was introduced in an adapted Technology Acceptance Model, to underscore the priority of use over the awareness of the scope of digital threats by Nigerian journalists. A line of discourse was also opened on the subject of the security threats that the media audience 'indirectly' pose. The following measures were thus recommended for the Nigerian journalists who form the focal point of this study: awareness of technology scope, technical support, personalised network, prompt action, and discreetness.

Keywords: Digital Security, Journalism, Technology, Threat, Audience

INTRODUCTION

Afolabi (2015) captures the essence of security as the presence of peace, safety, gladness, and the protection of human and physical resources or absence of crisis or threats to human dignity, all of which facilitate development. He also highlights seven dimensions of secuity *viz.* economic security, food security, health security, environmental security, personal security, community security, and political security. Today's journalist is invariably a digital-media reliant worker, no matter how minimal his or her reliance on digital media is. Consequently, journalists are exposed to the hazards of the digital workspace more often than they are aware of.

According to a UNESCO report in 2018, "journalists facing threats to their physical safety have been found to be particularly vulnerable to digital threats, and they are often unable or unwilling to take steps to mitigate digital risk." This state of affairs can be attributed to the basic-at-best digital training that most journalists have in respect to digital security, whereas the perpetrators of cybercrimes are typically tech-savvy and sophisticated in their knowledge of digital security and how to exploit it. Although Afolabi (2015) did not include "digital security" in the dimensions of security, it is a growing area of concern in today's digital, fast-paced, Internet era, and it impinges directly on the dimension of personal security.

METHODOLOGY

The study employed exploratory research design, while using literature review as a research instrument. Analysis of secondary data collected from reviewed literature, internet resources, and library materials, formed the basis for discussion of subjects raised in this study.

CONCEPTUAL FRAMEWORK

These are the definitions of key terms used in this paper:

Digital: Using or characterised by computer technology (Merriam-Webster Dictionary, 2024)

Safety: Freedom from the occurrence or risk of injury, danger, or loss (Collins Dictionary, 2024)

Security: The state of being away from hazards caused by deliberate intention of humans to cause harm (Selcuk, 2015)

Digital Footprint: The unique trail of data that a person or business creates while using the Internet (IBM)

Threat: An expression of intent to injure or punish another (Oxford English Dictionary, 2024)

Risk: Someone or something that creates or suggests a hazard (Merriam-Webster Dictionary, 2024)

Cybercrime: Crime committed using computer networks (Oxford English Dictionary, 2024)

21ST CENTURY JOURNALISM IN NIGERIA AND UNRECOGNISED THREATS

Attempts at mass communication in the pre-colonial era in Nigeria had their limits and were often set within the confines of a cultural group (Ogwezzy, 2021). The colonial era and the influx of western technology exposed Nigeria and Africa at large to media technology that transcends cultural and geographical limitations. To summarise the timeline of the technological transitions that shaped Nigeria's media in colonial and post-colonial times, the print media was the genesis, with the first known publication issued on December 3, 1859 (Akinfeleye & Okoye, 2003). The publication, a bi-lingual newspaper by the name *Iwe Irohin Fun Awon Ara Egba Ati*

Yoruba was published by Henry Townsend, an Anglican missionary from England, in a small printing press he set up in Abeokuta.

The next technology of mass media to follow in Nigeria was the radio, with the establishment of Radio Diffusion Service (RDS) in 1933; and the television, with the establishment of Western Nigerian Television (WNTV, now Nigerian Television Authority (NTA)) in 1959. The Internet-based media was the last to join the train, with the first online newspaper in Nigeria, *Post Express* (now defunct), which went online in 1997 (Akoh, 2012, as cited in Oladosu, Olusegun, & Tanimowo, 2021). As of today, all these forms of mass media are still existent in Nigeria, howbeit differently affected in their revenue streams and business models by the advent of the Internet.

While the influence of the Internet on traditional media business models is not the crux of this paper (Ali, Faridah, Mohd, & Maizatul (2011) and Chan-Olmsted (2004) already shed light on this area in their works), the influence of the Internet on business models necessitated the drift towards digital journalism that now characterises the mode of operation of nearly every media house in Nigeria today (Dunu, Ukwueze, & Ekwugha, 2017). In Dunu, Ukwueze, & Ekwugha (2017), digital media use by Nigerian journalists was recorded at a high rate of 92.8%. While other studies along the same line conducted on different samples reflect lower rates of digital media use by Nigerian journalists, the consensus is that digital media use characterises the business operation of most Nigerian media houses today.

Davis' 1989 Technology Acceptance Model explains the adoption rates of digital media technology variously observed. While the model accounts for "perceived usefulness" and "perceived ease-of-use," it does not account for "perceived threat of use" in its schema. "Perceived threat of use" is employed here to conceptualise the awareness by a user of

technology, of the risks associated with using that technology. If this was introduced into the Technology Acceptance Model, it would influence technology adoption as presented in Figure 1.

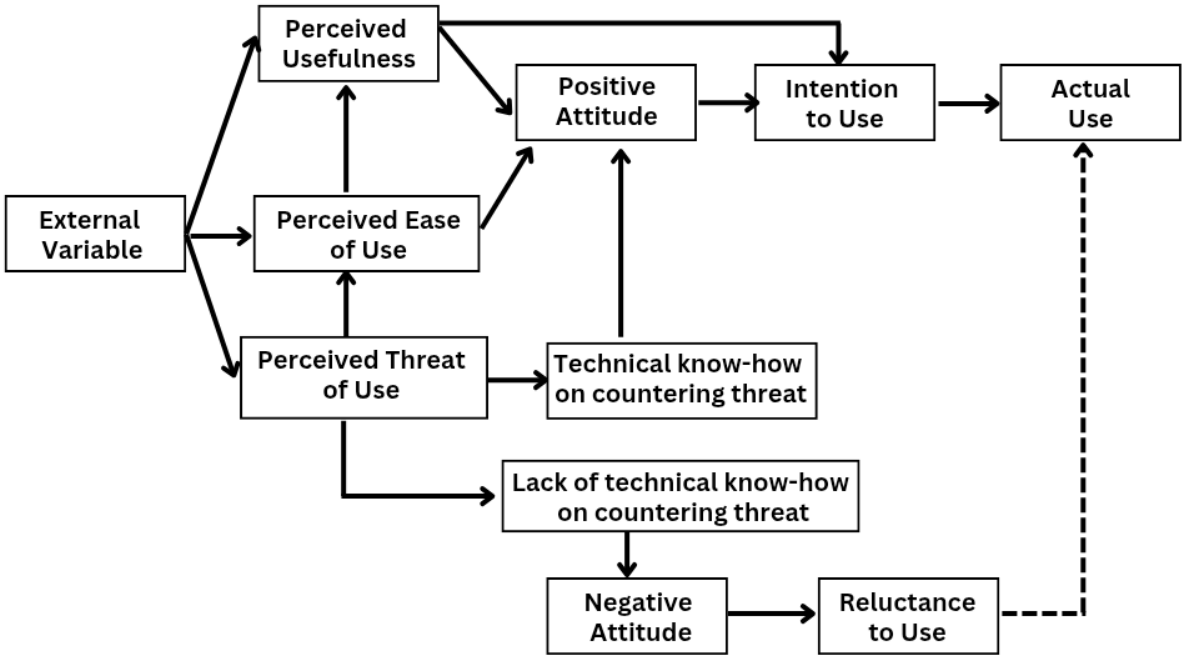

Figure 1: Technology Acceptance Model (adapted) | Source: Author

As this paper seeks to establish, the use of digital technology by Nigerian journalists, despite its security threats, and their lack of technical expertise in countering the threats, is due largely to their lack of the knowledge of existence of these threats, or their underestimation of what these threats could mean to their personal security, even when they are aware of the threats. Similarly, in cases where the journalist possesses "perceived threat of use" knowledge and lacks the technical expertise to counter the threat, use of technology is not totally declined, particularly when the "perceived usefulness" outweighs the "perceived threat of use." This explains the upward arrow between "perceived threat of use" and "perceived ease-of-use" in the adapted model of the Technology Acceptance Model in Figure 1. Other factors may be responsible for

this state of affairs, such as a sense of 'corporate security' at the work place, lack of firsthand knowledge of a cybercrime victim, and perceived powerlessness despite knowledge of threat; but those factors are not the focus of this paper.

To resolve some of the questions that can be raised from this discourse, a research in this area can adopt the objectives to:

i. examine the perception of Nigerian journalists on digital footprint and its attendant threats;
ii. ascertain the level of awareness on digital security measures among Nigerian journalists; and
iii. establish past experiences of Nigerian journalists with cyber-related crimes.

DIGITAL FOOTPRINT IN JOURNALISM

Kaku (2024) explains the categorisation of digital footprints into active and passive footprints. Active footprints are data trails that the user is directly and consciously responsible for, such as posts on a social media site or a blog page, uploaded content, etc. On the other hand, passive footprints are the data traces collected without the user's direct intervention, including IP addresses, search history, and cookies. It is these passive footprints that perpetrators of cyber threats often exploit. According to Jamal & Zain (2022), the three main digital footprint components subject to cyber attack are cache, cookies, and linkability. Essentially, users become susceptible by visiting websites, downloading files, exchanging e-mails (particularly with unverified sources), uploading content, and a host of other related online activities. E-mail use, chatrooms, online discussion forums, IP call/Voice over Internet Protocol (VoIP), and virtual conference (Skype or WhatsApp video call), among digital tools used by Nigerian journalists, are identified by Guanah & Omorinola (2018). These tools form an overlap with other digital tools where both passive and active digital footprints are logged.

The dilemma of choosing between a non-digital news business model at the risk of falling behind competitors in a fast-paced news environment, and a digital-assisted/full digital-based work mode that exposes journalists to online hazards and digital threats is made simpler by the argument advanced in Marshall McLuhan's technology determinism theory. The thrust of this theory argues that the society is influenced and shaped by technological development, and that the society has to adjust and adapt to new technologies and innovations (Baran, 2002). In essence, digital technology use has come to stay in journalism and the society at large, and journalists have to live up to coping with the downsides.

The digital trail left by journalists and the invasion of their privacy that cybercriminals can prey on via this digital trail predisposes the journalists to security threats in the following ways: their office or home location could be approximated using information from their IP address, thus exposing them to threat of physical harm; their banking details could be phished and their accounts emptied or splurged on unauthorised transactions; links with family members could be established and used as a blackmail tool; sensitive information acquired in confidence from sources could be breached; malware could be introduced into the journalist's computer, smart phone, or other digital devices, thereby compromising important files; a multiplatform bullying attack could be launched against the journalist through their personal accounts, to harass them into suppressing or expressing certain news stories; personal social media accounts of journalists could be hacked and used to post embarrassing or implicating content; contact details could potentially be exploited and used to intercept communication between the journalists and their contacts; and private information about the journalist could be published online with malicious intent (an act known as doxing).

REMEDYING THE EXPOSURE CHALLENGES

There is an increase in the level of cybercrime recorded in developing countries, including Nigeria, in the past two decades (Ghelerter, Wilson, Welch, & Rusk, 2022). This period overlaps with the period of increased Internet penetration in developing countries. *Global Digital Insight* reports it at a rate of four percent annually (about two hundred and eighty million people) (ibid). As the Internet penetration continues over the coming decades, the sophistication of Internet-based crimes is likely to increase also, and given technology determinism at play, journalists are not likely to relent in their use of digital technologies either. There is, therefore, the need for journalists to gain enlightenment on measures to stay safe from the increasing rate and complexity of cybercrimes. Ghelerter, Wilson, Welch, & Rusk (2022) noted that the developing world has yet to catch up with the developed world regarding cybersecurity. The huge financial investment to close the gap was a reason cited.

Notwithstanding, a number of measures can be put in place given the current resources that journalists in Nigeria work with as noted earlier: e-mail, chatroom, online discussion forums, IP call/Voice over Internet Protocol (VoIP) and virtual conference. These resources are accessed through Internet-enabled smartphones, tablets, desktop or laptop computer, and in recent times, smart watches. Electronic banking (including bank apps and ATM card) can also be a substrate for cyberattack. The following recommendations can be adopted as measures against cybersecurity threats faced by Nigerian journalists:

Awareness. Journalists are wont to apply technology to their work even when they do not fully comprehend the scope of the technology. They should therefore seek a general level of awareness about the security measures applicable to the technologies they use.

Consultation. Ideally, a technical support person should be affiliated with or employed by media houses, to tackle suspicious activities noticed by journalists on their account(s). This technical support person should also serve as a form of seasonal security update coach, to bring journalists up-to-speed on emerging scams and threats.

Personalised network. Use of a shared or public network, even among members of the same organisation can predispose users to data leakage and identity theft (Alaa, Tarek, & Tarek, 2021). While the cost of personal data subscription may far outweigh the perceived threat of use by many journalists and discourage them from spending personal finances on it, they may reserve such personal Internet connection for when very sensitive activities like bank transactions and confidential dialogues are to be carried out.

Prompt action. Cichonski, Millar, Grance, & Scarfone (2012) state that in the event of a data breach (real or suspected), quick response is critical. Journalists employing digital tools should not put off telltale signs of a data breach or compromised network till later. For every second spent not acting to contain the threat, more havoc may be wreaked by the cybercriminal behind the fraudulent actions.

Discreetness. As much as journalists have an identity to project and also deserve to enjoy their personal lives off-the-job, discretion should be applied when making posts on social media that could compromise their security, if exploited. An example is the posting of geo-tagged images while on vacation (geotagging allows other Internet users to know the location where a picture was taken). A more discreet approach with minimal and only relevant social media posting is recommended. Additionally, journalists should not hint at details of their location realtime, except it is linked to their journalistic assignment.

AUDIENCE AS QUASI-THREATS

Generally, individual and corporate success in the media industry are mapped by the audience size that can be pulled. The celebrity journalists all around the world are invariably people who command large audience following. While it is easy to think of threat-prone journalists in relation to the source of the threat, the audience is not a neutral factor in the 'threat cycle.' In a sense, a journalist who cannot boast of wide audience following is himself not a threat and can attract no threat to himself. Much of existing literature on security, like the ones cited in this study, identify various sources of threats to journalists. Khan & Dad (2020) additionally identifies family members of journalists as possible threats, where the murders of Pakistani women journalists who refused to give up a career in journalism was cited. However, the audience, if considered as pitching journalists in the limelight where threat becomes possible, they (the audience) ultimately have to be given roles to play in safeguarding the journalists. This line of thought could drive a future area of research, particularly as Khan & Dad (2020) has reported that the threats journalists face are rapidly changing and becoming increasingly complex.

CONCLUSION

Threats posed to journalists are increasing by the day. This study has reviewed the contribution of digital technology use by journalists and the unique security concerns they pose to the worsening security situation faced by Nigerian journalists. Measures are recommended to combat the digital security concerns at the level of sophistication that journalists in Africa (including Nigeria) currently operate. The role of audience in the security dynamics of journalists was also raised in a cursory manner to spur possible future research.

REFERENCES

Afolabi, M. (2015). Concept of Security. *Readings in Intelligence & Security Studies*, 1-11.

Akinfeleye, R., & Okoye, I. (2003). *Issues in Nigerian Media History*. Malthouse Press Limited.

Alaa, Z., Tarek, M., & Tarek, E.-H. (2021). Privacy Issues of Public Wi-Fi Networks. In Z. Alaa, M. Tarek, & E.-H. Tarek, *Advances in Intelligent Systems and Computing* (pp. 656-665).

Ali, S., Faridah, I., Mohd, Y., & Maizatul, H. (2011). The Impact of New Media on Traditional Mainstream Mass Media. *The Innovation Journal: The Public Sector Innovation Journal*, 2-10.

Baran, S. (2002). *Introduction to Mass Communication: Media Literacy and Culture.* Mayfield Publishing Co.

Chan-Olmsted, S. (2004). Introduction: Traditional Media and the Internet: The Search for Viable Business Models. *The International Journal on Media Management*, *6*(1&2), 2-3.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide.* National Institue of Standards and Technology.

Dunu, I., Ukwueze, C., & Ekwugha, U. (2017). What Effect? An Appraisal of Journalists' Use and Perception of New Media. *Online Journal of Communication and Media Technologies*, *7*(4), 179-198.

Ghelerter, D., Wilson, J., Welch, N., & Rusk, J.-D. (2022). Cybercrime in the Developing World. *2022 KSU Conference on Cybersecurity Education, Research and Practice.* Kennesaw State University.

Guanah, J., & Omorinola, O. (2018). The utilization of new media technologies in journalism practice in Delta State, Nigeria. In *Mass Communication Education and Practice in Nigeria* (pp. 174-195). Ahmadu Bello University Press Ltd.

IBM. (n.d.). *What is a digital footprint?* Retrieved from IBM: https://www.ibm.com/think/topics/digital-footprint#

Jamal, N., & Zain, J. (2022). A Review on Nature, Cybercrime and Best Practices of Digital Footprints. *2022 International Conference on Cyber Resilience (ICCR).*

Kaku, S. (2024). Navigating the Digital Landscape: Understanding and Managing Your Digital Footprint. *Global Media Journal*, *22*(68), 1-3.

Khan, S., & Dad, N. (2020). Threats Against Journalists. *Global Conference for Media Freedom* (pp. 1-7). Digital Rights Foundation.

Oladosu, I., Olusegun, A., & Tanimowo, O. (2021). Trends and Patterns of Online Newspapers in Nigeria: A Study of Sahara Reporters and the Premium Time. *International Journal of Research and Innovation in Social Science (IJRISS)*, *5*(3), 499-506.

Ogwezzy, A. (2021). *African Communication Systems II.* National Open University of Nigeria (NOUN).

Selcuk, N. (2015). The Definitions of Safety and Security. *Journal of ETA Maritime Science*, *3*(2), 53-54.

UNESCO. (2018). *World Trends in Freedom of Expression and Media Development.* University of Oxford.