f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Digital footprints in non-digital environments: How publicly displayed information invades the right to privacy

by Gregory Gondwe

Abstract

This study explored the relationship between publicly displayed information and the right to privacy in Zambia and Tanzania. The purpose was to examine whether the behavior displayed by individuals in public environments reveals and undermines their quest for the right to privacy. I asked participants to observe and document the type of clothing an individual wore, the logos or monograms on their clothing or bags, and words spoken in public. This information was then used by Google to identify individuals online. Findings suggest that there is still a disconnect between what people display in non-digital and what they post on social media. However, there is also a growing trend of people leaving a trail of digital footprints that relate to their publicly displayed behaviors.

Contents

Introduction

The right to privacy in the digital age has become a recurring theme in most scholastic discourses (Adams, 2020; Kperogi, 2022; Papadopoulou and Maniou, 2021; Swart, *et al.*, 2018). However, there remains a dearth of research on the relationship between how much information we consciously choose to expose online versus how that information is protected by the laws of privacy. Against the conscious-raising 2018 Cambridge Analytica scandal that cemented the importance of individual privacy on social media (whether one is consciously doing it), is the question of how individuals unwillingly expose their privacy in non-digital environments.

The link between the two is that people's non-digital lives today cannot be separated from their digital lives. As Klonick (2019) noted, "Ubiquitous technology such as search engines on a smartphone in the hands of a stranger can compromise our privacy in our everyday lives". Klonick performed an experiment with her students to determine what public information strangers displayed and whether that information

could invade their privacy. The experiment required students to determine a stranger's identity in a public place using only Google searches on their mobile phones. Students were asked to base their search on publicly displayed information such as things strangers said loudly, clothing, bags, logos, and monograms. To their amazement, the students found that they were able to identify a stranger based on publicly displayed information. This suggests that neither the public nor private life can claim to be unadulterated.

Research into the right to privacy has a long-standing history, yet there is still a scarcity of literature addressing the emerging challenges posed that are accompanied by new media. For example, scholars and lawyers are still grappling with the ongoing trial in which Vanessa Bryant opened a case against Los Angeles County over the graphic images of the crash that killed her husband, Kobe Bryant, and their daughter. Essentially, the widow is suing the County for negligence and invasion of privacy, while asserting that she suffered emotional distress. In this 'privacy trial', some pundits have questioned how the lawyers would justify the legal underpinnings given that, the accident occurred in a public space, the victims were celebrities, and the same victims are deceased. However, this is not to undermine the value of ethics in this conundrum.

Therefore, this study draws from similar insights and replicates Klonick's (2019) study, but in an African setting. Essentially, I examined whether people in Zambia and Tanzania could be digitally identified through their non-digital, publicly displayed environments. I asked whether the information we display in public is sufficient to identify us via the Internet. Even so, how much information do people in Zambia and Tanzania post online? And to what extent can that information be used to collect their private information? This study sought to examine whether the African environment shares commonalities with the West in what they display on social media versus their non-digital daily lives. I ask about the extent to which individuals in Zambia and Tanzania can be identified through Google search engines by looking at their publicly displayed lives. Consistent with Klonick's (2019) approach, I examine what strangers said aloud in public, their clothing, their logo, and/or monograms. This paper provides a context for engaging with the idea of privacy in publicly displayed activities while showcasing innovative contributions to the swiftly emerging body of research in the area.

Literature review and theory

Privacy as a social concept

Despite emerging as a present-day issue, the notion of privacy is deeply embedded in the early history of civilization [1]. Warren and Brandeis' (1890) quest for the right to privacy cemented the desire to be left alone. In their seminal article, "The right to privacy", Warren and Brandeis expressed concern about new technological innovations of the time and their abilities to invade one's privacy. Notably, "the advent of instant photography and audio recordings allowed the media to profit on the most prurient interests without care of the caused harm" (Warren and Brandeis, 1989). Therefore, Warren and Brandeis argued for the extent to which common law could accommodate one's right to be left alone; thus, identifying the harm predicated on mental anguish and feelings — which, in and of themselves, were an actionable right to protect (Coudry and Mejias, 2019; Mbembe, 2019; Vimalkumar, *et al.*, 2021).

Central to these arguments is that many existing laws, though implying the right to privacy, continue to attenuate the right to one's personality, peace of mind, or even the right to be left alone. As Bycer (2014) posits:

> While slander and libel would stop false representations, they bore no way to stop an invasion of private facts. Copyright law that could protect individual letters had become inadequate/obsolete with the rapidly evolving technology that

> could disgorge one's privacy without stealing or copying any tangible items. Rights in property, and even to the exclusive right to control publication of one's labor, could not express the privacy rights in their entirety, as no property is physically divested. Contract law would not go far enough. A judicial declaration of public morality, private justice, and general convenience would not support a finding for breach of confidence in an implied contract if there were no prior relation between the parties. Criminal law could not be used to enforce privacy rights absent specific legislation that would allow the State to intervene in a "private" civil matter.

Brycer's (2014) statement suggests that the legal implications of a privacy case are only determined by how one uses information and how lawyers justify their claim over an invasion of privacy. One hundred years after Warren and Brandeis' provocative piece, debates have continued and are now exacerbated by unprecedented new media developments. Most of these debates are girded by notions of whether publicly exposed life should be protected. The recent case of Vanessa Bryant in which she was awarded US$16 million over crash photos taken of Kobe Bryant and her daughter Gianna, attests to the existing conundrum. Until today, whether public information should be protected by law, remains a question of ethics. This is because the right to privacy continues to be firmly ingrained in the common law. In the U.S., for example, publicly displayed information is not protected under the laws of privacy in the sense that you cannot sue someone for taking a photograph of you in public. But you could challenge them about the ethics of doing that and the underlying implications. In the case of Vanessa Bryant, emotional distress sufficed for invasion of privacy — but one would also argue that you need very good lawyers and probably fame to win such a case.

Critiques have emerged to challenge the right to privacy phenomenon. Accordingly, they argue that the idea of privacy is predicated on one's state of solitude, intimacy, anonymity, and reserve, by which a high state indicates a higher level of privacy and vice versa (Westin, 1967). This implies that the amount of information disclosed by an individual should be the criteria for determining the degree to which one needs to be left alone [2]. But, to what extent is this plausible? Is it possible to attain optimal degrees of privacy? Research suggests otherwise (Katzav, 2022), given the many variables that surround our environments. Ultimately, this boils down to the principle that one's publicly displayed life is not protected by the laws of privacy. If one decides to expose some information about themselves, that information becomes public, *i.e.*, you cannot take one to court for taking your picture in a public place (bar, beach, public transportation, streets, etc.). However, one can appeal for consideration to the conscious of the person taking a photo.

The law of privacy in sub-Sahara Africa

The law of privacy varies across societies, in the sense that one's value of privacy is correlated with the weight that society places on privacy as a right. Even in sub-Saharan Africa, the ideas of privacy are determined by cultural underpinnings (Olinger, *et al.*, 2007). For example, privacy in South Africa is not understood in the same way as privacy in Zambia or Tanzania. But even in Zambia, privacy in the eastern part is not the same as privacy among people from the southern or western parts of the same country. This is because of the different cultural underpinnings, *i.e.*, dress codes, gestures, etc. For example, while some cultures are okay with exposing women's breasts in public, other cultures find that offensive and an invasion of privacy. But when it comes to the laws governing privacy, most African states continue to mimic those of the West in the sense that there are no specific laws designed to protect one's right to be left alone. This idea is also supported by the fact that African communities are communal in nature. Therefore, the idea of being left alone is almost non-existent.

However, most constitutions in Africa have adopted the recent Data Protection and Privacy Act laws that have emerged in the wake of the Internet. Person data means "an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person" [3]. Essentially, the Act applies to the processing of personal data performed through automated and/or electronic means. This provision limits the processing of data when such an Act will fundamentally affect other rights and freedoms.

While this definition sounds all-encompassing, its scope is limited to data extracted by automated and electronic means. And like most acts, the Data Protection and Privacy Act is accompanied by derogations and other forms of language that limit the extent to which an individual can claim that their privacy has been invaded. In countries that have adopted the Data Protection and Privacy Act, for example, some clauses suggest that the "Act does not apply to the processing of personal data by an individual for personal use". [4] Yet the constitutions fail to define the meaning of individual or personal use, thus opening a wide array of opportunities for individuals who would use the processing of data as "for personal use" to defend their deviant motives.

Additionally, most Data Protection and Privacy Acts are followed by a provisional clause of exemption in the case of national security. Given that most African countries have been accused of using national security as an excuse to suppress freedom, it is suspicious that a government could claim a need to invade one's right to privacy. Other limitations to this include a lack of cross-border limitations, questions of data retention, and the control of data protection commissioners whose offices lack independence from the government. Above all, there is a lack of defined strategies for implementing the Act, especially since online data is still in its stage of infancy in most African countries. Mostly, the data that is prone to misappropriation is derived from social media. That is where most Africans post what is real or fake about their lives.

However, information found in bank accounts, social security numbers, and many other identifying kinds of information have not yet been connected online. It is recently that individuals have been required to provide detailed information like the National Registration Card (NRC) numbers to register for a mobile phone number. In fact, even the National Registration Cards are yet to be digitalized except for a few passport holders and probably those who have acquired birth certificates. The trend is different in most Western countries where most individual data are interconnected within online networks; *i.e.*, a birth certificate, social security number, criminal charges, for example, are connected to mobile, bank, school, or even medical accounts. Given the interconnectedness of valuable data in the West, it is explainable why Klonick's (2019) study provided key elements of identifying one through publicly displayed information.

Because of unclear regulations in the Data Protection and Privacy Act, individuals and corporations in Zambia and Tanzania have continued to misappropriate online data for their own gains. Although the Acts have been implemented, little or no effort has been made to educate the majority of Africans about them. For example, there is no identifiable case in Zambia or Tanzania where an individual sued a fellow individual or corporation for invasion of privacy. Photos and videos of people involved in accidents, children, and other individuals in most need have been violated, yet little or no effort has been dedicated to addressing and educating communities about the right to privacy. Ultimately, this suggests that despite the Data Protection and Privacy Act, the notion of privacy is still governed by ethics and not legal implications of a given case. In other words, there is clear evidence to suggest that publicly displayed information is governed by ethics as opposed to law in both the West and sub-Saharan Africa (Basimanyane, 2022; Makulilo, 2016; Namara, *et al.*, 2018). This means that one cannot receive legal punishment for invading publicly displayed behavior. As a result, regulating privacy in most diverse societies is still complex. Even the idea of the Data Protection and Privacy Act (DPPA) remains a challenging endeavor.

Law of privacy as a theoretical phenomenon

Theoretically, privacy can be better understood in terms of Altman's (1975) concepts of personal space, territoriality, and crowding. Although Altman employed a social psychological framework, his approaches impinge on many other disciplines including media and communication. Altman (1975) defines privacy as "a set of interpersonal boundary-control processes which paces and regulates the interaction with others"

[5]. This boundary process is regulated by an ability to manage interpersonal interactions (Pedersen, 1999) — in that the contact is both restricted and sought. To gain optimal privacy, Altman believed that verbal and paraverbal behavior had to take precedence in controlling personal space, claiming territory, and negotiating cultural norms with society [6]. Against this background, Altman proposed "an optimal degree of desired access of the self to the other at any moment in time" [7]. As Tufekci (2008) continued to argue, "a state of perfect privacy would be akin to a state of absolute solitude, which is not only undesirable but also the harshest modern judicial punishment short of the death penalty". These statements suggest that optimal privacy is only attained when one has the ability to control privacy, *i.e.*, not coerced but independently electing to either be alone or with people even when surrounded by a crowd (Basimanyane, 2022).

But most environments we live in are interdependent in the sense that one has to forfeit some privacy for the sake of the other. For example, individuals have a strong sense of privacy in 'private environments', such as residential homes. But the fact that they live in a community with communal expectations, their privacy is defined within the circles and needs of that community. In communal societies, even residential homes are not common. Take for instance rural areas of Zambia where most people do the same things together. It is almost impossible that one can sleep in unless they are sick. If one does not show up by 8:00 AM, people become worried and go to check on them. Although not specifically describing the incidence of privacy, such environments have limitations to how much one could be left alone.

Until the twentieth century, privacy was never a legal right. Today, U.S. laws describe it in terms of four distinct areas: Intrusion — the unwarranted violation of one's physical solitude; Publicity of embarrassing private facts; publicizing information that puts one in a false light; and appropriation — using a person's name, picture, or likeness without permission, usually for commercial exploitation. Protection only occurs when one invades privacy that an individual has been making an effort not to make private. For example, everyone has the right to privacy in their private environment. However, once they relinquish all their privacy on purpose, or made it public, only ethics can save them [8]. Hence public figures and celebrities have difficulties protecting their privacy. Many countries have no explicit laws to protect a right to privacy. Essentially most derive the right to privacy from other laws, *i.e.*, the "freedom to associate" clause of the First Amendment in the U.S.; Limitations on searches and seizures (Fourth Amendment); limitations on disclosure of personal information (Fourteenth Amendment); and others in the Third and Fifth Amendments that respectively protect against the quartering of soldiers and self-incrimination.

Nonetheless, little or no form of effort is dedicated to protecting privacy in public environments. Hypothetically, implementing such limits would infringe upon the freedom of others. There is the basic assumption that individuals are careful not to expose their privacy to the public. What about the right to be left alone? What if one wants to enjoy a moment of solitude in a public case? As Altman (1975) argued, the idea that people can conceal their private information just because they are in public is utopian. This is because: "People will assume anonymity in public and then reveal various levels of private information given what they believe their environment to be, and what tools might be available to manage disclosure" (Klonick, 2019). This observation has become more prevalent today in the digital age where information is stored and registered digitally. This means that one does not need to relinquish privacy to others to access it. Knowingly and unknowingly, one leaves behind digital footprints that others can access and use for personal gain.

How easy is it to access such information? According to Klonick's example, it is easy to access personal and private identities through legal means. Based on her experiment, this can easily be done by observing what one is wearing, noting logos on clothing, what is said in public, and other clues. Therefore, this study attempted to test the same experiment in a different context and environment. The purpose was to examine whether people in Zambia and Tanzania could also be digitally identified through their non-digital, publicly displayed environments. Overarching, I asked the following questions:

> *RQ1a*: What is the relationship between publicly displayed behavior and digital footprints among individuals in public

spaces in Zambia and Tanzania?

Rationale: This question attempts to situate the relationship between what information individuals in Zambia and Tanzania choose to display in public and how that information can be used to identify and collect private data. In this case, we are looking at ordinary citizens who, to a large extent, are protected by law. Second, I am interested in everyday information that one chooses or inevitably displays. For example, it is inevitable that one would wear some clothing although the kind is also determined by either choice or ability to choose. On the other hand, there is the push for one to display private information in public even when their intention is not to. This assumption is supported by Altman (1975) who argued that there was a thin line between what we want to keep private and how we choose to protect that information. Accordingly, he asserted that individuals will generally assume anonymity in public and then reveal various levels of private information given what they believe their environment to be and what tools might be available to manage disclosure. This technique is used in police interrogations. The police might choose to leave someone in solitude while watching them. Even when these individuals understand that they are surrounded by cameras, they tend to exhibit other forms of behavior that might reveal guilt or innocence.

RQ1b: To what extent is individual privacy in Zambia and Tanzania accessible online through publicly displayed information?

Rationale: This *RQ* sought to examine whether individual private lives can be correlated to publicly displayed information. For example, is there a relationship between one's dress code and what one posts online? In the U.S. people do not just wear clothes with brands. One who is wearing a Lakers' jersey, for example, is likely associated with the team. Similarly, one does not just wear a hoodie from a particular state unless they have links to that state. This is a little different in most countries that rely on second-hand clothing from Western countries. If this is the case, therefore, to what extent can one be identified through clothing, logos, or monograms?

Methods

Sampling

This study followed Altman's (1975) observational approach to social problems. Since the study employed human subjects, IRB approval was sought and issued on 28 May 2022. Thereafter, I used WhatsApp groups to reach out to 271 individuals to participate as observers in Zambia and Tanzania. Of the 271, 185 observers were former high school classmates and 32 were former college mates from Zambia. The remaining 81 former college mates were from Tanzania. Of the 271 participants, 67 were female. This is

because participants from Zambia were recruited from single-sex schools. Therefore, to account for gender balance, we only recruited other males, thus providing us with a total of 134 possible observers to help with the study. To ensure gender balance, we first recruited female respondents, who among the 67, 43 were willing to participate. Of the male respondents, 38 confirmed their participation, thus providing us with a total of 81 confirmed participants. The participants comprised different social statuses, including graduate and undergraduate students, members of the working class, people engaging in business, farmers, and the unemployed, to name a few. The mean age of the participants was 28 years. In each group, the participants entered a US$50 raffle ticket.

Each observer was asked to observe and record publicly displayed information only. Using collected information, an observer searched for a person on Google and Facebook. To avoid confusion, observers were asked to select one location which they frequented the most. The locations included bars, restaurants, commuter buses, open markets, and *vigiweni/gazebos*, where most people in the communities spend time chatting (Note: *vigiweni*/gazebos are places where most people go to hang and chat about anything. In Tanzania, *vigiweni* denotes a huge rock in which people can sit aimlessly and chat about almost anything. Today, especially in Tanzania, people go to *vigiweni* for cheap street coffee and chat about community issues and politics. Most people have criticized such gatherings as breeding laziness because they do nothing other than chat. We avoided places such as schools and churches and considered them private. A minimum of 15 people were assigned to each category. Reliability checks were performed using content analysis of 10 random observations from each category.

Data analysis

All observations were documented in the form of words, phrases, or sentences. This is because each observer was asked to document what they observed in public spaces. Two transcripts representing Zambia and Tanzania were created for analysis and uploaded to Nvivo, a software package used for computer-assisted qualitative text analysis. Then, I coded each transcript using a list of themes compiled from discussion summaries prepared by each observer. I iterated the coding and included other themes that emerged during this process. Outside input from the observers was also sought to confirm the validity of the coding and to identify areas of discrepancy. Data from both Zambia and Tanzania were later organized into three key themes that reflected the research questions and their accompanying rationale. The generated themes include the relationship between clothing and digital identity, Speech/language/spoken words and digital identity, and social behavior vs. digital identities (Social behavior in this case referred to unspoken actions that an individual exhibits. It could be through dance, the music they seemed to approve or enjoy, how they reacted to some instances, (*i.e.*, were their actions driven by particular emotions or beliefs?), or personal character (*i.e.*, introvert versus extrovert).

Findings

The relationship between clothing and digital identities

Based on the information collected from five locations, we were able to demonstrate that there was no substantial relationship between what people wore, logos on their clothing, monograms, etc., and their digital identities. Essentially, most individuals wore clothing with labels from the U.K. (*i.e.*, soccer jerseys) and the U.S., with inscriptions such as California, NYC, Texas, and Dallas. Additionally, there was no information suggesting that these individuals had visited these places. However, such labels might be used to define one's social status, given that most clothes are second-hand, or simply known as *salaula* in Zambia or *mitumba* in Tanzania (Hansen, 1999). As a side note, most people of lower-class status wear second-hand clothing or cheap brands from China.

Nonetheless, certain clothes and labels were used to identify the affiliations of some individuals. This was

particular to the kind of soccer teams they supported, such as Manchester United, Chelsea, Liverpool, Arsenal, etc. However, such information cannot be fully used to search and find information on Google or social media platforms. Against this backdrop, few individuals could be identified by their clothing. This is especially true for those who wore their work clothes, such as individuals working in the mines in Zambia, police officers, bank workers, etc. Most of these individuals had names printed on their clothing.

The relationship between conversations and digital identities

The findings suggest that most people revealed their identities in conversations. According to the data collected, many individuals expressed their positions on a soccer team that they supported, their political parties of affiliation, their religion, and sometimes their workplaces. Most of this information was collected from bars, commuter buses, and *vigiweni*, where people freely debate topical issues. With publicly displayed information, observers were able to find some individuals online by searching some of key terms or claims that were made. However, identifying identities by conversation is not easy. It requires a painstaking connection to publicly displayed information. In other words, a single statement is insufficient to identify someone. When one connected the dots, one could trace them. Some observers reported how people talked about their places of work, bosses, schools, qualifications, and so on, which correlated with what most people posted on their social media accounts.

Relationship between social behavior vs. digital identity

Social behavior, in this case, refers to unspoken actions that an individual exhibits in public environments. Most of these behaviors were connected to community behavior, and how one amplified them as an individual. Some examples were dance, the music one seemed to approve or disapprove of, how one reacted to some situations or personal character — that is, introvert versus extrovert. The data suggested that social behavior partially accounted for identifying one online. For example, how one responded to certain circumstances determined education level, the soccer teams that they supported, and their religious, political, and other social affiliations. On the other hand, their extrovert levels, that is, one could easily stand and start dancing to a song playing on the radio, exhibited information that could be traced back to them. For example, in Tanzania, one was able to locate someone's identity by searching for the location and the kind of dance that they exhibited. It was found that other people had taken photos of the person earlier and posted them on social media. In addition, comments disclosed the person's identity, where they grew up, and what they currently do. However, similar to other forms of identification, this requires a painstaking process of connecting different kinds of clues.

Discussion and conclusions

This study draws from Klonick's (2019) experiment and class exercise to examine relationships between publicly displayed behavior and privacy in Zambia and Tanzania. The purpose was to explore whether individuals reveal private information through publicly displayed behavior. Our findings partially support this hypothesis. These findings are inconsistent with Klonick's (2019) experiment; however, this study provides an essential standpoint for interrogating our right to privacy.

The findings suggest that with effort and intention, one can find a correlation between individual publicly displayed behavior and online details. These findings are consistent with the arguments made by Altman (1975). Altman (1975) asserted that "people will assume anonymity in public and then reveal various levels of private information given what they believe their environment is and what tools might be available to manage disclosure". Altman believed that it was almost impossible to conceal privacy given the environment and available tools. Most studies have established this by observing information posted online. However, these findings present a new perspective suggesting that even ecological environments reveal what we seek to conceal. Klonick's (2019) experiment attests to this phenomenon; however, our findings

reveal some variations.

Several factors can be attributed to variations observed in this study. The first is the extent of Internet use in Africa. While most countries in Africa are now interconnected, there is still a disconnect between digital platforms and what is displayed in non-digital environments. Unlike in Western countries, it is almost impossible to find students on their university Web sites. This is because many organizations continue to operate outside the Internet. Even police records are still traditional, unlike in the United States. Most banks, too, although going digital, are not yet on the Internet in the sense that one cannot strictly perform a digital transaction. However, there are what we would consider digital transactions, such as mobile money, which, in a strict sense, operates within technology but under a single model of mobile broadband. In short, it is almost impossible to search for someone based on their mobile money transactions because they are not connected to the general Internet, even when they utilize certain Internet technologies.

Second, unlike most people from the West, most Africans distinguish themselves from the media. In other words, people in most African countries perceive the media and its programing as isolated from their lives. This is because most media tend to report stories of the elite few while ignoring issues that pertain to the majority (Wasserman and Boloka, 2004). Gondwe (2018) attributed this trend to the history of the media in Africa, which served colonial masters, and subsequently elite politicians. Today, people are reintegrating with media through social media participation. Wwhile we observe a partial correlation between what individuals do in their private lives and what they do in public, we could also argue that the next generation might be more connected to the media than the current generation. This is because the current generation was not born within the technological era as with the West. For instance, people in the U.S. who were born at least 25 years ago had access to the Internet, played video games, and most probably owned cell phones at an early age. This experience is only happening today in Africa but not to everyone.

What, then, is the relationship between publicly displayed information and digital footprints among individuals in public spaces in Zambia and Tanzania? Klonick (2021) would ask. I argue that, while in the West we should be concerned about ramifications, Africa's cases are at their infancy stage. Therefore, such a realization offers avenues for Africa to clearly prepare itself for challenges related to privacy. In other words, Africa has the opportunity to learn from the West and the implications that the phenomena have posed on the right to privacy. However, whether this problem can be remedied remains an unexplored endeavor that requires further research. All in all, this study contributes to two strands of the right to privacy in an African setting: The phenomena of privacy in publicly displayed information, and the understanding of how publicly displayed information affects the private information that we seek to protect. Future research may explore the currently enacted laws on Data Protection and Privacy Act (DPPA). While these are important, their complexity and effects remains unexplored. FM

About the author

Gregory Gondwe is an assistant professor of Journalism Studies at California State University, San Bernardino.
E-mail: gregory [dot] gondwe [at] csusb [dot] edu

Notes

1. Solove, 2006, p. 481.

2. Katzav, 2022; Wanjugu, 2020, p. 39.

3. See, for example, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-is-personal-data/.

4. https://www.dataguidance.com/notes/zambia-data-protection-overview#:~:text=In%20terms%20of%20material%20scope,an%20individual%20for%20personal%20use.

5. Altman, 1975, p. 10.

6. Tufekci, 2008, p. 21.

7. Altman, 1975, p. 11.

8. Bivins, 2003, p. 149.

References

P.C. Adams, 2020. "Agreeing with surveillance: Digital news privacy policies," *Journalism & Mass Communication Quarterly*, volume 97, number 4, pp. 868–889.
doi: https://doi.org/10.1177/1077699020934197, accessed 7 September 2023.

I. Altman, 1975. *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, Calif.: Brooks/Cole.

D. Basimanyane, 2022. "The regulatory dilemma on mass communications surveillance and the digital right to privacy in Africa: The case of South Africa," *African Journal of International and Comparative Law*, volume 30, number 3, pp. 361–382.
doi: https://doi.org/10.3366/ajicl.2022.0414, accessed 7 September 2023.

T. Bivins, 2003. *Mixed media: Moral distinctions in advertising, public relations, and journalism*. New York: Routledge.
doi: https://doi.org/10.4324/9781410609045, accessed 7 September 2023.

M.L. Bycer, 2014. "Understanding the 1890 Warren and Brandeis 'The right to privacy' article," *National Juris University*, at https://nationalparalegal.edu/UnderstandingWarrenBrandeis.aspx, accessed 4 September 2023.

N. Couldry and U.A. Mejias 2019. "Data colonialism: Rethinking big data's relation to the contemporary subject," *Television & New Media*, volume 20, number 4, pp. 336–349.
doi: https://doi.org/10.1177/1527476418796632, accessed 7 September 2023.

G. Gondwe, 2018. "When party policies do not matter: Examination, the ambivalence of voting behaviors in the Zambian presidential elections," *African Journal of Political Science and International Relations*, volume 12, number 1, pp. 10–21.
doi: https://doi.org/10.5897/AJPSIR2017.1052, accessed 7 September 2023.

K.T. Hansen, 1999. "Second-hand clothing encounters in Zambia: Global discourses, western commodities, and local histories," *Africa*, volume 69, number 3, pp. 343–365.
doi: https://doi.org/10.2307/1161212, accessed 7 September 2023.

G. Katzav, 2022. "Compartmentalised data protection in South Africa: The right to privacy in the Protection of Personal Information Act," *South African Law Journal*, volume 139, number 2, pp. 432–470, and at https://journals.co.za/doi/full/10.47348/SALJ/v139/i2a8, accessed 7 September 2023.

K. Klonick, 2019. "A 'creepy' assignment: Pay attention to what strangers reveal in public," *New York Times* (8 March), at https://www.nytimes.com/2019/03/08/opinion/google-privacy.html, accessed 7 September 2023.

F.A. Kperogi (editor), 2022. *Digital dissidence and social media censorship in Africa*. London: Routledge. doi: https://doi.org/10.4324/9781003276326, accessed 7 September 2023.

A.B. Makulilo, 2016. "The context of data privacy in Africa," In: A.B. Makulilo (editor). *African data privacy laws*. Cham, Switzerland: Springer, pp. 3–23. doi: https://doi.org/10.1007/978-3-319-47317-8_1, accessed 7 September 2023.

A. Mbembe, 2019. Necropolitics. Translated by S. Corcoran. Durham, N.C.: Duke University Press. doi: https://doi.org/10.1215/9781478007227, accessed 7 September 2023.

M. Namara, D. Wilkinson, B.M. Lowens, B.P. Knijnenburg, R. Orji, and R.L. Sekou, 2018. "Cross-cultural perspectives on eHealth privacy in Africa," *AfriCHI '18: Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, article number 7, pp. 1–11. doi: https://doi.org/10.1145/3283458.3283472, accessed 7 September 2023.

H.N. Olinger, J.J. Britz, and M.S. Olivier, 2007. "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa," *International Information & Library Review,* volume 39, number 1, pp. 31–43. doi: https://doi.org/10.1080/10572317.2007.10762729, accessed 7 September 2023.

L. Papadopoulou and T.A. Maniou, 2021. "'Lock down' on digital journalism? Mapping threats to press freedom during the COVID-19 pandemic," *Digital Journalism*, volume 9, number 9, pp. 1,344–1,366. doi: https://doi.org/10.1080/21670811.2021.1945472, accessed 7 September 2023.

D,M. Pedersen, 1999. "Model for types of privacy-by-privacy functions," *Journal of Environmental Psychology*, volume 19, number 4, pp. 397–405. doi: https://doi.org/10.1006/jevp.1999.0140, accessed 7 September 2023.

D.J. Solove, 2006. "A taxonomy of privacy," *University of Pennsylvania Law Review*, volume 154, number 3, pp. 477–564. doi: https://doi.org/10.2307/40041279, accessed 7 September 2023.

J. Swart, C. Peters, and M. Broersma, 2018. "Shedding light on the dark social: The connective role of news and journalism in social media communities," *New Media & Society*, volume 20, number 11, pp. 4,329–4,345. doi: https://doi.org/10.1177/1461444818772063, accessed 7 September 2023.

Z. Tufekci, 2008. "Can you see me now? Audience and disclosure regulation in online social network sites," *Bulletin of Science, Technology & Society*, volume 28, number 1, pp. 20–36. doi: https://doi.org/10.1177/0270467607311484, accessed 7 September 2023.

M. Vimalkumar, S.K. Sharma, J.B. Singh, and Y.K. Dwivedi, 2021. "'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants," *Computers in Human Behavior*, volume 120, 106763. doi: https://doi.org/10.1016/j.chb.2021.106763, accessed 7 September 2023.

S.N. Wanjugu, 2020. "Privacy relinquishing and safeguarding: When are consumers willing to disclose or protect their information?" *Doctor of Business Administration (DBA) dissertation, Louisiana Tech University*, at https://digitalcommons.latech.edu/dissertations/880/, accessed 7 September 2023.

S.D. Warren and L. Brandeis, 1989. "The right to privacy," In: T. Goldstein (editor). *Killing the messenger: 100 years of media criticism*. New York: Columbia University Press, pp. 1–21.

S.D. Warren and L. Brandeis, 1890. "The right to privacy," *Harvard Law Review*, volume 15, number 5,

pp. 193–220.
doi: https://doi.org/10.2307/1321160, accessed 7 September 2023.

H. Wasserman and M. Boloka, 2004. “Privacy, the press and the public interest in post-apartheid South Africa,” *Parliamentary Affairs*, volume 57, number 1, pp. 185–195.
doi: https://doi.org/10.1093/pa/gsh015, accessed 7 September 2023.

A.F. Westin, 1967. *Privacy and freedom*. New York: Atheneum.

Editorial history

Received 10 April 2023; revised 15 June 2023; accepted 4 September 2023.

Digital footprints in non-digital environments: How publicly displayed information invades the right to privacy
by Gregory Gondwe.
First Monday, volume 28, number 9 (September 2023).
doi: https://dx.doi.org/10.5210/fm.v28i9.12837