

Beyond the resume: perceptions of cybervetting among employees in Nigeria

by

Uzoma Stanley Chukwuebuka

B.A., University of Benin, 2019

A THESIS

submitted in partial fulfillment of the requirements for the degree

MASTER OF SCIENCE

A.Q. Miller School of Media and Communication
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2026

Approved by:

Major Professor
Dr. Sean Eddington

Copyright

© Stanley Uzoma 2026.

Abstract

Cybervetting, the practice of evaluating job candidates based on their online presence, has become a prominent component of global recruitment. However, existing research is heavily Western-centric, leaving a critical gap in understanding how employees in the Global South, especially in sub-Saharan Africa, interpret and experience these digital screening practices. This qualitative study explores how Nigerian employees perceive cybervetting, the underlying factors influencing their views, and how these interpretations are shaped by cultural dimensions as conceptualized in Geert Hofstede's Cultural Dimensions Theory.

Drawing on semi-structured interviews with 14 Nigerian professionals from diverse industries, the findings reveal that employees perceive cybervetting as an extension of organizational control that collapses personal-professional boundaries, disrupts contextual privacy, and introduces a high risk of misjudgment. Employees do not uniformly accept or reject the practice; instead, they actively negotiate its legitimacy based on platform type, job relevance, and transparency. Furthermore, the study identifies that an employee's acceptance is heavily structured by economic positioning, the broader institutional normalization of data access in Nigeria, and moral framings of personal responsibility.

Through a cultural lens, the research indicates that while a collectivist orientation can legitimize cybervetting as a means of protecting organizational reputation, high power distance does not translate into unconditional acceptance of employer surveillance. Ultimately, the study introduces the theoretical concept of "pragmatic privacy compliance," illustrating how individuals may outwardly comply with privacy-invasive practices due to economic and structural pressures while internally resisting them. These insights offer significant implications

for employees and job applicants, as well as human resources practitioners and policymakers, aiming to design fair, transparent, and ethically grounded cybervetting policies.

Table of Contents

List of Tables	vii
Acknowledgements	viii
Chapter 1 - Introduction.....	1
Chapter 2 - Literature Review.....	3
The Emergence and Evolution of Cybervetting	3
Employers' Perspectives on Cybervetting.....	5
Employees' Reactions and Perceptions of Cybervetting.....	6
Cross-Cultural Variations in Cybervetting Perceptions.....	8
Theoretical Framework: Geert Hofstede's Cultural Dimensions Theory.....	10
The African Context: A Research Gap	15
Chapter 3 - Methodology	17
Research Design	17
Participants and Sampling	17
Participant Profile	19
Data Collection	20
Interview Protocol.....	21
Data Processing and Analysis.....	21
Data Validity and Trustworthiness	23
Peer Debriefing	23
Thick Description.....	24
Positionality Statement	24
Chapter 4 - Findings.....	26
RQ1.How do employees in Nigeria perceive Cybervetting, particularly regarding issues of privacy and fairness?	27
Cybervetting Extends Organizational Control Beyond Workplace Boundaries.....	27
Collapse of Personal–Professional Boundaries	28
Disruption of Contextual Privacy	29
Extension into Surveillance	30
Cybervetting Produces Interpretive Uncertainty and Risk of Misjudgment.....	31
Collapse of Contexts	32
Fixing Identity Across Time	33
Employees Actively Negotiate Legitimacy of Cybervetting Across Contexts.....	35
RQ2: What factors influence employees' perceptions of cybervetting practices?	37
Economic Positioning Conditions the Expression of Privacy Beliefs	38
Institutional Normalization of Data Access as a Structural Factor	41
Moral Framing of Responsibility as a Factor Shaping Acceptance.....	42
RQ3: How do cultural dimensions or values, such as collectivism, power distance, and uncertainty avoidance, shape the interpretation of cybervetting?.....	44
Collectivist Orientation as a Basis for Legitimizing Cybervetting	44
Power Distance and the Limits of Cybervetting Legitimacy	47
Uncertainty Avoidance and Resistance to Cybervetting Ambiguity	48
Chapter Summary	50

Chapter 5 - Discussion	52
Theoretical Contributions	52
Cybervetting as a Dynamic and Contextually Negotiated Practice	53
Structural Shaping of Cybervetting Perceptions	54
Revisiting Power Distance: Authority, Legitimacy, and the Limits of Compliance	56
Practical Implications	58
Limitations and Future Research	59
Conclusion	63
References	66
Appendix A - Interview Protocol.....	75
Power and Questioning Management	77
Rules, Policies, and Uncertainty	78
Appendix B - Consent Form	79
Appendix C - Appendix: IRB Approval Letter.....	83

List of Tables

Table 1: Demographic and Occupational Characteristics of Participants	19
---	----

Acknowledgements

It is often said that it takes a village to raise a child; this project is a child that was nurtured by many people, to whom I owe deep appreciation.

First and foremost, I am deeply thankful to my advisor, Dr. Sean Eddington, whose guidance, patience, and insight were invaluable at every stage of this work. His encouragement and thoughtful feedback consistently pushed me to think more critically and strengthen my research.

I am also grateful to my committee members, Dr. Samuel Mwangi and Dr. Raluca Cozma, for their time, helpful suggestions, and careful feedback during my prospectus defense, all of which contributed greatly to improving this thesis.

My sincere thanks go to all the participants who took part in this study, as well as those who helped spread the word and assisted in recruiting others. Your support made this research possible.

I would also like to acknowledge my peers and colleagues, whose conversations, collaboration, and friendship made this journey both intellectually enriching and genuinely enjoyable. Thank you, Sherifa, Sultana, and Doyin, for making my time at K-State so memorable.

Finally, I am especially grateful to my family—my parents, Daniel and Grace, and my siblings, Chibuike, Esther, and Ogochukwu. Your love, encouragement, and constant support mean everything to me. This milestone would not have been possible without you.

Chapter 1 - Introduction

In today's increasingly digital world, cybervetting has become a common component of recruitment processes globally (Jacobson & Gruzd, 2020). Cybervetting, also known as internet surveillance, social media background checks, online screening, social media profiling, or even "Facebook fired," refers to the practice of evaluating job candidates based on their online presence (Berkelaar & Harrison, 2017). With the advancements in communication technologies, employers can now conduct a simple Google search to find a job applicant's social media profiles and may even carry out more in-depth analyses of their digital footprints across multiple platforms (Jacobson & Gruzd, 2020). Reflecting this growing trend, CareerBuilder (2018, as cited in Jacobson & Gruzd, 2020) reported that the use of cybervetting had surged from 11% to 70% within a decade, highlighting organizations' increasing reliance on social media and other online data when screening candidates.

Although cybervetting may offer employers an efficient way to assess candidates beyond their résumés, it also raises critical concerns about fairness, consent, and the blurring lines between personal and professional boundaries (Akbulut et al., 2024; Berkelaar, 2017). While this trend has been extensively studied in Western contexts, less is known about how it is experienced in the Global South, particularly in countries like Nigeria, where digital access and social media use are rapidly expanding. As of December 2023, Nigeria boasted approximately 163.8 million internet subscribers, reflecting a 9.07% increase from the previous year (BusinessDay, 2024). This surge highlights the country's accelerating digital transformation and growing online engagement, further emphasizing the increasing significance of online presence in various aspects of life, including employment. As employers in Nigeria adopt cybervetting

practices, employees and job seekers are faced with new challenges regarding privacy and self-presentation.

Existing research on cybervetting has largely focused on Western contexts; as a result, far less is known about how employees in the Global South—particularly in Sub-Saharan Africa, such as Nigeria—interpret and evaluate cybervetting practices. This gap is significant given the distinct cultural values, economic conditions, and power dynamics that shape these contexts. To address this gap, this study draws on in-depth interviews with Nigerian employees and applies Geert Hofstede’s Cultural Dimensions Theory as an analytic lens to examine how employees perceive cybervetting and how cultural and contextual factors shape these perceptions.

Beyond its scholarly contribution, the study also has practical significance for employers and human resources practitioners in Nigeria and similar contexts by informing the design of transparent, fair, and ethically grounded cybervetting policies.

Chapter 2 - Literature Review

This chapter reviews existing literature on cybervetting to provide a foundation for the study. It begins with the emergence and evolution of cybervetting, tracing how the practice has developed over time. It then examines employer perspectives, followed by employee reactions and perceptions. The chapter next explores cross-cultural variations in how cybervetting is understood and evaluated. It also outlines the theoretical framework, drawing on Geert Hofstede's Cultural Dimensions Theory to guide the analysis. Finally, the chapter identifies the African context as a key research gap and presents the research questions that inform this study.

The Emergence and Evolution of Cybervetting

Cybervetting has emerged alongside the rapid expansion of digital communication technologies and the increasing integration of the internet into everyday social and professional life. Early hiring practices relied primarily on formal application materials, interviews, and reference checks. However, the rise of social networking platforms such as LinkedIn, Facebook, and Twitter in the mid-2000s significantly expanded the volume and accessibility of personal information available to employers, fundamentally altering how candidates can be assessed (Berkelaar, 2014; Davison et al., 2012). As a result, employers gained the ability to access informal, user-generated content that extends beyond the carefully curated materials traditionally submitted during the hiring process.

By the early 2010s, cybervetting had become increasingly institutionalized as part of recruitment and selection practices. Survey-based research indicates that a substantial proportion of employers began incorporating social media screening into hiring decisions, with estimates ranging from nearly half to over two-thirds of hiring professionals engaging in some form of online screening (Society for Human Resource Management [SHRM], 2016; CareerBuilder,

2018). This growth has been driven in part by the perceived advantages of cybervetting, including its low cost, ease of access, and potential to provide additional insights into candidates' personalities, behaviors, and organizational fit (McDonald et al., 2021). In this sense, cybervetting is often framed as a logical extension of existing selection practices, enabled by technological innovation and increasing data availability.

At the same time, the emergence of cybervetting reflects broader transformations in the employment relationship and expectations surrounding professional identity. As digital platforms blur the boundaries between personal and professional life, individuals are increasingly expected to manage their online presence in ways that align with organizational norms and expectations (Berkelaar, 2014; Gershon, 2017). This shift has contributed to the normalization of online screening, as both employers and job candidates come to anticipate that social media content may be accessed and evaluated as part of the hiring process. Consequently, cybervetting is not merely a technological development but also a social and organizational phenomenon shaped by evolving norms around visibility, transparency, and self-presentation in the digital age. Despite its widespread adoption, cybervetting remains a relatively recent and still-evolving practice. Research continues to highlight its informal and often unregulated nature, with many organizations lacking clear policies or standardized procedures governing how online information should be used in hiring decisions (McDonald et al., 2021; Wilcox et al., 2022). This lack of institutionalization contributes to ongoing debates about the legitimacy, fairness, and ethical implications of cybervetting, positioning it as a contested practice rather than a fully established component of personnel selection. As such, understanding the historical emergence of cybervetting is essential for situating contemporary discussions of employee perceptions within a broader context of technological change and shifting organizational expectations.

Employers' Perspectives on Cybervetting

A growing body of research examining employer perspectives shows that cybervetting is understood as both a strategic and interpretive practice shaped by organizational goals and subjective evaluation processes. McDonald et al. (2021) explain that employers often justify cybervetting as a pragmatic tool for reducing hiring uncertainty, verifying applicant information, and assessing organizational fit, particularly in contexts where traditional application materials are perceived as insufficient.

Extending this perspective, qualitative studies highlight the interpretive nature of cybervetting in practice. For instance, Hedenus et al. (2021) show that recruiters actively examine candidates' online social networks to infer forms of social and cultural capital, using digital connections and interactions as indicators of employability, professionalism, and trustworthiness. Similarly, a recent qualitative study by Albishri et al. (2025) finds that hiring professionals view cybervetting as an increasingly integral component of digital talent acquisition, used to gather supplementary information beyond formal application materials. Recruiters reported analyzing candidates' social media profiles to identify both positive and negative behavioral cues, including indications of professionalism, personality, and value alignment.

Rather than serving solely as a tool for verification, cybervetting emerges as an interpretive process through which employers evaluate candidates' character and perceived organizational fit based on online content. Unlike resumes and interviews, which are often carefully curated by applicants, social media profiles are perceived to offer more "authentic" insights into an individual's personality, behavior, and values (Berkelaar & Buzzanell, 2015;

Gruzd et al., 2020). This perceived authenticity underpins the belief that cybervetting can enhance hiring decisions by revealing traits that may not emerge in formal evaluation contexts. Cost-efficiency and accessibility further reinforce the appeal of cybervetting. Compared to formal background checks, reviewing publicly available online information is relatively inexpensive, quick, and easy to integrate into existing hiring workflows (McDonald et al., 2021). In this sense, cybervetting is often positioned as a practical solution to time and resource constraints in recruitment processes.

However, not all hiring agents or managers fully endorse cybervetting. Some express ambivalence toward the practice, questioning the accuracy of social media data while also raising ethical and legal concerns related to privacy and potential discrimination (Wilcox et al., 2022). Some of these employers and managers caution that cybervetting may inadvertently introduce bias into hiring processes, as online profiles can reveal protected characteristics such as race and gender, increasing the risk of unequal treatment. For them, cybervetting highlights a central paradox: although it is intended to reduce organizational risk, it may instead generate new risks, including diminished applicant trust, reduced organizational attractiveness, and potential legal liability.

Employees' Reactions and Perceptions of Cybervetting

Job seekers themselves often react negatively to cybervetting, viewing it as an intrusive measure that violates personal boundaries (Cook et al., 2020; Roulin & Liu, 2023). Research indicates that while applicants might acknowledge the potential benefits of social media in the job search process, they express apprehension about invasive screening methods (Rózsa & Kmecová, 2020). A consistent finding across studies is that many job seekers react adversely to being cybervetted without consent. In early seminal research, Stoughton et al. (2015) found that

U.S. job applicants who learned a prospective employer had reviewed their Facebook profile overwhelmingly perceived it as an invasion of privacy, leading to diminished organizational attractiveness. Approximately two-thirds of participants in their study reported a negative view of the employer due to feeling their privacy was violated. Notably, this negative reaction persisted regardless of whether the applicant ultimately got the job, indicating that even successful candidates harbored distrust if they knew their social media was screened. Such findings suggest that cybervetting can undermine initial trust in organizations. It may also deter high-quality candidates (“elite prospects”) who “are more likely to steer clear of potential employers they don’t trust.” Furthermore, applicants who felt wronged expressed greater intent to pursue legal action for privacy invasion, underscoring the strong moral outrage induced by covert cybervetting.

These reactions reflect a broad consensus: employees and applicants often feel that cybervetting oversteps acceptable boundaries, especially when it involves personal social networks. Importantly, not all individuals react identically. Stoughton et al. (2015) reported that personality traits moderated reactions: candidates low in agreeableness were most offended by social media checks, perhaps due to lower tolerance for norm violations. Nonetheless, the overall pattern of perceived injustice is clear. From the employee perspective, undisclosed cybervetting clashes with expectations of privacy and fairness in the hiring process (akin to covert surveillance). Research by Berkelaar and Buzzanell (2015) further found that job seekers prefer to know if and how employers are examining their online information, rather than having it done “behind the scenes.”

Additionally, perceptions of fairness regarding cybervetting practices vary considerably across social media platforms, with applicants feeling more scrutinized on personal sites

compared to professional ones like LinkedIn (Balcerak et al., 2023). For instance, a study conducted in Germany by Schäpers et al. (2025) found that cybervetting carried out on professional platforms such as LinkedIn was associated with higher perceived fairness, lower perceived invasion of privacy, and greater organizational attractiveness compared to screening on personal platforms. However, even when cybervetting is conducted on professional platforms, non-job-relevant cues, such as photos, hobbies, or personal interests, can still influence recruiters' judgments, thereby raising ongoing fairness and validity concerns (Sallach et al., 2024).

Cross-Cultural Variations in Cybervetting Perceptions.

While negative sentiment about privacy invasion is common, acceptance of cybervetting can vary across cultural and national contexts. Most empirical studies to date have focused on Western populations, but limited evidence from other regions suggests cultural norms significantly influence perceptions. For example, Gruzdt et al. (2020) conducted a comparative survey of job seekers in the United States and India, guided by Communication Privacy Management theory. They found a striking difference: respondents in India were significantly more comfortable with employers screening their social media than were respondents in the U.S. No gender differences emerged in either country, implying privacy expectations around cybervetting may be governed more by culture than by demographic traits.

The authors attribute the U.S.–India gap partly to broader cultural orientations: the U.S. is often characterized as an individualistic culture with higher privacy concerns, whereas India's collectivist context might foster different privacy norms. Indeed, prior studies show Indians tend to report lower overall concern about online privacy compared to Americans. In collectivist or high-context societies, people may be more accustomed to blurred personal-professional spheres

or assume that organizations have a right to certain personal information as part of a social contract. Moreover, differing legal and social media landscapes matter – in India (until recently), the regulatory framework for data privacy was less stringent than in, say, Europe, potentially affecting expectations. Thus, comfort with cybervetting is not uniform worldwide; it is filtered through cultural lenses. What one society deems a gross privacy violation, another may see as a reasonable precaution or even an expected practice.

Beyond India, emerging research in other non-Western settings echoes both commonalities and context-specific nuances. A recent two-part study in Turkey (Akbulut et al., 2024) explored employer and employee perceptions of cybervetting in a metropolitan Turkish context. The authors note that past research was “largely conducted with Western samples,” highlighting a need to investigate different cultural settings.

In the first part of the study, interviews with Turkish hiring managers revealed a spectrum of attitudes toward cybervetting. Some expressed reservations about using social media to screen candidates, citing concerns about the relevance and reliability of online information. They questioned whether the content found online was truly job-related or accurate enough to inform hiring decisions. Ethical concerns also surfaced, particularly regarding the invasion of privacy, as many felt that delving into candidates’ personal online lives was inappropriate. Additionally, doubts about the validity of such assessments and the potential for bias—especially in interpreting ambiguous content—contributed to their hesitation.

Conversely, other hiring managers viewed cybervetting as an essential tool in the modern hiring process. They described it as a necessary form of due diligence, particularly in an age where online presence is ubiquitous. These managers believed that social media profiles could reveal authentic traits and behaviors that might not emerge during formal interviews.

Furthermore, cybervetting was seen as a useful method for consistency checking, helping to verify the accuracy of resume claims and identify potential red flags or discrepancies in a candidate's background. This dichotomy shows an ongoing debate: some employers (and by extension, employees when they put themselves in the employer's role) view cybervetting as an unfair intrusion, while others see it as a useful, even indispensable, tool.

In the second part of the study, Akbulut et al. surveyed 316 Turkish employees about their feelings on cybervetting and found perceptions tied to notions of organizational justice. The perceived fairness and face validity of cybervetting correlated positively with organizational justice attitudes. In other words, if employees believed that social media screening was a legitimate and relevant part of hiring (high "face validity"), they were more likely to view the employer's hiring process as fair overall. This suggests that contextual acceptance – or lack thereof – can impact broader impressions of an organization's fairness. Interestingly, consistent with the North American and Indian studies, gender was not a differentiator in Turkey; male and female employees shared similar views on cybervetting's acceptability. This convergence across disparate contexts (U.S., India, Turkey) that gender plays little role hints that privacy boundary expectations might be shaped more by cultural and individual experiences than by gender socialization.

Theoretical Framework: Geert Hofstede's Cultural Dimensions Theory

This study is grounded in Geert Hofstede's Cultural Dimensions Theory, which provides one of the most influential frameworks for understanding how cultural values shape individual behavior and organizational practices across societies.

Initially developed through a large-scale survey of IBM employees in over 50 countries, the theory identifies key value dimensions that differentiate national cultures and influence

communication, decision-making, and perceptions of authority (Hofstede, 1983). Subsequent refinements expanded the original four dimensions to six, providing a more comprehensive understanding of cultural variability (Hofstede, 2011; Minkov & Hofstede, 2012). The model remains widely applied in communication, management, and psychology research due to its strong empirical base and explanatory power (Kirkman et al., 2006; Taras et al., 2010; Beugelsdijk et al., 2017).

At its core, Hofstede's framework posits that national cultures differ systematically along six value dimensions: power distance, individualism versus collectivism, uncertainty avoidance, masculinity versus femininity, long-term versus short-term orientation, and indulgence versus restraint. Each dimension reflects deeply embedded social values that guide how individuals relate to authority, manage uncertainty, balance personal and group interests, and define appropriate social behavior.

Power distance (PDI) refers to the extent to which individuals in a society accept and expect unequal distributions of power (Hofstede, 2011). In high power-distance cultures, hierarchy is viewed as natural and desirable, and subordinates are less likely to question authority. Conversely, in low power-distance societies, people prefer equality and participative decision-making. Research consistently shows that power distance influences leadership expectations, perceptions of fairness, and tolerance for surveillance in organizations (Kirkman et al., 2006).

Individualism versus collectivism (IDV) captures whether individuals view themselves primarily as autonomous agents or as members of cohesive social groups. Individualistic cultures emphasize independence, privacy, and self-expression, whereas collectivist cultures value loyalty, group harmony, and relational obligations (Hofstede, 1983; Hofstede, 2011). Empirical

evidence indicates that this dimension is particularly predictive of workplace behaviors, communication preferences, and attitudes toward privacy (Taras et al., 2010).

Uncertainty avoidance (UAI) describes the degree to which members of a culture feel uncomfortable with ambiguity or unpredictable situations. Societies high in uncertainty avoidance prefer structured rules, formal procedures, and stability, whereas low uncertainty-avoidance cultures are more open to change and ambiguity (Hofstede, 2011). This construct is central to understanding how people evaluate risk management and rule enforcement within organizations (Kirkman et al., 2006).

The masculinity versus femininity (MAS) dimension distinguishes between cultures that prioritize competitiveness, achievement, and material success (masculine) and those that emphasize care, cooperation, and quality of life (feminine) (Hofstede, 2011). Although originally framed in gendered terms, this dimension reflects societal values around assertiveness and nurturance, influencing reward systems, conflict resolution, and organizational culture.

Long-term versus short-term orientation (LTO) reflects whether a culture values perseverance, future planning, and thrift (long-term) or respect for tradition, social obligations, and maintaining one's reputation (short-term). Introduced through cross-cultural studies in East Asia, this dimension highlights differences in temporal perspectives and adaptability (Minkov & Hofstede, 2012).

Finally, indulgence versus restraint (IVR) describes the degree to which societies allow gratification of basic human desires for enjoyment and leisure versus suppressing such gratification through strict social norms (Hofstede, 2011). Indulgent cultures tend to emphasize personal freedom and happiness, while restrained societies favor social order and self-discipline.

Despite its enduring influence, Hofstede's framework has been subject to substantial criticism regarding its methodology, assumptions, and applicability to contemporary global contexts. One major critique concerns its methodological foundations. The original model was based solely on data from IBM employees, raising concerns about sample bias and the representativeness of findings for entire national cultures (McSweeney, 2002). Scholars argue that the reliance on a single multinational corporation's workforce limits the theory's generalizability, as it may reflect organizational culture as much as national culture (Minkov & Kaasa, 2021).

Another limitation involves the assumption of cultural homogeneity within nations. Critics contend that Hofstede's framework treats countries as uniform cultural entities, overlooking significant intra-national diversity based on ethnicity, region, class, or religion (McSweeney, 2009; Brewer & Venaik, 2012). This simplification risks stereotyping national cultures and underestimating local variations that influence behavior.

Further, scholars question the temporal stability of Hofstede's dimensions. As societies evolve under globalization and digital transformation, cultural values may shift more rapidly than Hofstede's static indices suggest (Taras et al., 2012; Minkov & Kaasa, 2021). The framework's limited capacity to capture dynamic cultural change challenges its ongoing relevance for modern, interconnected contexts.

Finally, critics highlight conceptual and measurement issues, including overlap between constructs and ambiguity in how dimensions are operationalized (Smith, 2006; Gerhart & Fang, 2005). For example, the interpretation of masculinity–femininity has been questioned for its gendered assumptions, and the metrics for long-term orientation have evolved over time, raising concerns about construct validity (Beugelsdijk et al., 2017).

In light of these limitations, many researchers advocate for using Hofstede's framework as a guiding heuristic rather than a definitive measure of culture (McSweeney, 2009; Minkov & Kaasa, 2021). When applied cautiously and complemented with qualitative or multi-level perspectives, the theory remains a valuable tool for examining how cultural values influence perceptions and attitudes in various social and organizational contexts.

A substantial body of empirical research has applied Hofstede's Cultural Dimensions Theory across diverse contexts, confirming its utility for explaining cross-national variation in organizational behavior and communication. Meta-analytic reviews by Kirkman et al. (2006) and Taras et al. (2010) suggest that Hofstede's dimensions reliably predict workplace attitudes, trust, and commitment across cultures, while Beugelsdijk et al. (2017) highlight the framework's continued relevance when applied with careful methodological alignment.

More targeted research illustrates how specific cultural dimensions influence perceptions of fairness and authority acceptance, which are crucial for interpreting individuals' responses to cybervetting. For instance, van den Bos et al. (2013) and Brockner et al. (2001) found that individuals in high power-distance cultures emphasize consistency over participatory "voice" when evaluating procedural fairness, whereas those in low power-distance settings value transparency and input. These findings suggest that employees in hierarchical cultures may view employer monitoring as more legitimate than those in egalitarian ones.

In technology and privacy research, Hofstede's constructs have been widely employed to explain cross-cultural differences in digital acceptance and data sensitivity. Srite and Karahanna (2006) and Straub et al. (1997) demonstrated that individualism, uncertainty avoidance, and masculinity influence willingness to adopt digital systems. Similarly, Bellman et al. (2004) and

Engström et al. (2023) found that countries high in individualism and uncertainty avoidance report stronger online privacy concerns.

While Hofstede's Cultural Dimensions Theory identifies six cultural dimensions, this study focuses on three—individualism–collectivism, power distance, and uncertainty avoidance—because they offer the greatest explanatory value for understanding employee perceptions of cybervetting. Individualism–collectivism helps clarify cultural variations in privacy expectations and personal–professional boundaries, power distance explains differing levels of comfort with employer authority and oversight, and uncertainty avoidance sheds light on tolerance for ambiguous or unregulated hiring practices. The remaining dimensions (masculinity–femininity, long-term orientation, and indulgence–restraint) are less conceptually central to the aims of this study and are therefore not emphasized. Collectively, these three dimensions form the primary theoretical lens through which cultural influences on employees' interpretations of cybervetting are examined. Concepts such as fairness and privacy are used as sensitizing concepts to guide the interpretation of participants' accounts of cybervetting experiences.

The African Context: A Research Gap

Overall, perceptions of cybervetting among employees and job applicants across the globe range widely. While some accept it as a normal and even necessary part of a transparent hiring process, others view it as an invasion of privacy and a breach of trust. Research highlights a general awareness of the practice. Despite this awareness, many individuals express discomfort, particularly when cybervetting extends into personal or non-professional content. A common sentiment is that context matters: just because information is publicly accessible does not mean it was meant to be used for professional evaluation.

A clear gap in existing research on cybervetting is the limited number of studies conducted in the Global South—particularly in Africa. While most empirical work has focused on North America and Europe, with some emerging research from Asia (e.g., India) and the Middle East/Eastern Europe (e.g., Turkey), African countries such as Nigeria remain largely unexplored in this area. This lack of research leaves important questions unanswered, especially given Nigeria’s distinct cultural, socioeconomic, and technological landscape. As a collectivist society with strong communal values, Nigeria also upholds unique norms around hierarchy, reputation, and information sharing. These factors are likely to influence how employees perceive employer scrutiny of their online presence in ways that differ from Western contexts. For instance, while Nigerian individuals may be more socially open due to community-oriented values, they may also place strong emphasis on respect and social hierarchy. In such a setting, a manager reviewing an employee’s social media profile could be seen either as a reasonable exercise of authority or as an intrusive act that violates personal boundaries. Without research grounded in the local context, such interpretations remain speculative.

Understanding these nuances requires focused, culturally aware studies within the region. Drawing from the reviewed literature and guided by Hofstede’s Cultural Dimensions Theory, this study seeks to explore the following research questions:

RQ1: How do employees in Nigeria perceive cybervetting, particularly regarding issues of privacy and fairness?

RQ2: What factors influence their perceptions of cybervetting practices?

RQ3: How do cultural dimensions such as collectivism, power distance, and uncertainty avoidance shape the way employees in Nigeria interpret and evaluate cybervetting?

Chapter 3 - Methodology

Research Design

This study adopted a qualitative research design to explore how Nigerian employees perceive cybervetting and the cultural and contextual factors shaping these perceptions. Given the context-specific nature of these experiences, a qualitative approach was well suited to uncovering participants' lived realities and the meanings they attribute to them. This approach facilitated a deeper understanding of the nuanced ways individuals interpret their experiences—insights that are not easily captured through quantitative methods (Creswell, 2013). It also allowed for flexibility in examining how cultural orientations, such as power distance, collectivism, and uncertainty avoidance, influence employees' interpretations of cybervetting practices. Overall, this design aligns with the study's aim of generating a rich, contextualized understanding of how culture shapes employees' attitudes toward cybervetting practices.

Participants and Sampling

A total of 14 participants were recruited using a combination of purposive and snowball sampling strategies. Purposive sampling enabled the selection of individuals with direct experience of cybervetting in the Nigerian workplace who could provide in-depth, reflective insights. It also facilitated the recruitment of participants across diverse industries, genders, and age groups, allowing for the exploration of potential variation in responses across different demographic and professional contexts. Snowball sampling complemented this approach by allowing initial participants to refer others within their professional networks who met the study criteria. This strategy was particularly appropriate given the sensitivity of the topic, as it facilitated access to participants through established trust networks when discussing issues such as digital surveillance, privacy, and workplace norms (Noy, 2008).

While an initial target of 8–12 participants was established, consistent with qualitative research guidelines on data saturation, a total of 14 participants were ultimately included in the study. A sample size within this range is widely considered appropriate for qualitative, in-depth interview studies aimed at exploring individual experiences and meaning-making processes, where the goal is thematic saturation rather than statistical generalization. Prior research suggests that saturation, the point at which no new themes emerge, can often be achieved within the first 6 to 12 interviews, particularly when participants share relatively similar experiences (Creswell, 2013; Guest, Bunce, & Johnson, 2006). Although thematic saturation was reached within the initial sample of 12 participants, two additional participants were purposefully recruited to address a gender imbalance, as women were underrepresented. This decision enhanced the demographic diversity of the sample and strengthened the study's ability to capture a broader range of perspectives.

Prior to recruitment, ethical approval was obtained from the Institutional Review Board (IRB) at Kansas State University to ensure that all study procedures met established ethical standards for research involving human participants. Please see Appendix C for details.

For recruitment, the researcher first developed a recruitment document outlining the purpose of the study and participant eligibility criteria. To be eligible for participation, individuals were required to (1) be currently employed in Nigeria or have been employed within the past 12 months, (2) use social media or maintain an active online presence, and (3) be aware of or have experienced employers reviewing social media during hiring, promotion, or as part of workplace policies. This document was shared with the researcher's contacts in Nigeria, primarily through the WhatsApp messaging application. Through this process, the initial set of participants was identified and recruited. Some of these participants subsequently assisted in

recruiting additional individuals who met the study criteria, consistent with the use of snowball sampling.

Following recruitment, participants were provided with an informed consent form detailing the study's purpose, procedures, confidentiality measures, and the voluntary nature of participation. All participants reviewed and signed the consent form electronically prior to participating in the study.

Participant Profile

This section provides an overview of the demographic and occupational backgrounds of the 14 participants included in this study. This information aims to contextualize participants' perceptions of social media screening and the factors shaping their interpretations.

To protect participants' confidentiality, each individual was assigned a pseudonym. Confidentiality was further maintained through the removal of identifying information from interview transcripts. Only the researcher had access to identifiable data.

Table 1: Demographic and Occupational Characteristics of Participants

Participants	Gender	Age	Education	Industry/Sector	Job Role
Hammie	Male	Late 20s	Bachelor's	Technology	Programmer
Eyo	Male	Early 30s	Bachelor's	Oil & Gas	Medical Officer
Kev	Male	Early 30s	Bachelor's	Banking/Finance	Banker
Kay	Female	Late 20s	Bachelor's	Real Estate	Realtor
Tee	Male	Early 30s	Bachelor's	Banking	Banker
Grand	Male	Early 30s	Bachelor's	Logistics	Manager
Kine	Male	Early 30s	Bachelor's	Travel Agency	Customer Support
Lee	Female	Early 40s	Master's	Insurance	Marketer
Zoe	Female	Mid-20s	Bachelor's	Fashion	Designer
Sel	Male	Mid-40s	Bachelor's	Oil & Gas	Engineering Support Officer
Ike	Male	Early 30s	Master's	Banking/Finance	Banker

Sunny	Male	Early 30s	Bachelor's	Religious Organization	Chief Security Officer
Kuni	Male	Late 20s	Bachelor's	Public Sector (Agriculture)	Civil Servant
Moe	Male	Late 30s	Bachelor's	Media/Publishing	Editor

Note. Age is reported in approximate categories to preserve participant confidentiality.

Data Collection

Data were collected through semi-structured interviews, which allowed for consistency across participants while also providing the flexibility to explore their perceptions, experiences, and interpretations in depth. Semi-structured interviewing is particularly effective for capturing rich, detailed accounts while maintaining a focused line of inquiry (Kallio et al., 2016).

All interviews were conducted in English, the official language of Nigeria. Given that participants had attained at least a college-level education, they demonstrated a strong command of the language and were able to express themselves clearly. During the course of the interviews, some participants engaged in code-switching between English and Nigerian Pidgin; these expressions were translated by the researcher to ensure accuracy in transcription and analysis.

Each interview lasted between 30 and 50 minutes, providing sufficient time to explore participants' experiences in depth while maintaining engagement. Interviews were conducted using either the WhatsApp video call feature or Zoom, depending on participant preference. The video recording function available on Zoom was used to record interviews when participants consented to video capture. While some participants were comfortable with full video recording, others preferred that only audio be recorded. For participants who expressed concerns about video recording, interviews were conducted in a manner that respected their preferences. In such

cases, the interview was conducted via WhatsApp video call on the researcher's computer, while audio was recorded separately using a mobile device.

In addition to audio recordings, field notes were taken during and immediately after interviews to capture participants' nonverbal cues, reactions, and overall demeanor. The inclusion of observational notes alongside interview data is widely recognized as enhancing the depth and credibility of qualitative research by providing contextual insight beyond verbal responses (Phillippi & Lauderdale, 2018)

Interview Protocol

An interview protocol was developed to explore participants' perceptions of cybervetting, particularly in relation to fairness and privacy, as well as the contextual factors influencing these perceptions. Questions were also designed to examine how cultural values, specifically collectivism, power distance, and uncertainty avoidance, shape participants' interpretations of cybervetting. Probing questions were used throughout to encourage elaboration and the sharing of concrete examples. Overall, the guide was structured to move from general perceptions to more specific experiences and reflections, allowing for both depth and flexibility in participants' responses. The full interview protocol, including all questions and prompts, is provided in Appendix A.

Data Processing and Analysis

Following the interviews, audio recordings were transcribed using the speech-to-text functionality available on the mobile device used for recording. The researcher subsequently reviewed each transcript manually to ensure accuracy and completeness. This step was particularly important because the speech-to-text feature was not always able to accurately

capture Nigerian Pidgin expressions (e.g., “shebi,” “wetin we dey talk,” “na so now”) used by some participants.

During this review process, the researcher corrected transcription errors, refined wording where necessary, and ensured that punctuation was appropriately applied. This manual verification and cleaning process helped to produce accurate and reliable transcripts for subsequent analysis.

All transcripts were securely stored in a password-protected folder on an encrypted cloud platform and labeled using pseudonyms to protect participant confidentiality. Any identifying information was removed during transcription. Access to this folder and any identifiable data was restricted to the researcher, and all data were used solely for academic purposes in accordance with Institutional Review Board (IRB) guidelines.

Data were analyzed using Sarah J. Tracy’s (2020) phronetic iterative approach, which involves a cyclical movement between inductive, data-driven analysis and theoretically informed interpretation. Analysis began with inductive open coding of interview transcripts to capture participants’ emic meanings, using descriptive and in vivo codes. At this stage, attention was paid to participants’ language, tone, and emphasis, particularly in how they framed and interpreted cybervetting practices. Analytic memos were written throughout this phase to document emerging insights, patterns, and reflexive considerations, including the researcher’s interpretations and evolving assumptions.

Initial coding generated a wide range of codes. As analysis progressed, codes were iteratively refined, merged, or organized into broader analytic categories through constant comparison across transcripts. The analysis moved between emic insights and etic frameworks,

linking emergent patterns to relevant theoretical concepts, including Geert Hofstede's Cultural Dimensions Theory and literature on fairness, privacy, and organizational surveillance.

The iterative process continued through successive rounds of coding and abstraction, during which patterns were examined and interpretations further developed. Analytic memoing remained central throughout, supporting ongoing reflexivity and helping to track the evolution of analytic decisions. The analysis involved sustained engagement with the data, moving back and forth between transcripts, codes, and theoretical frameworks to ensure that interpretations remained grounded in participants' accounts while being conceptually robust. This iterative approach enabled the development of nuanced, contextually informed insights into how Nigerian employees perceive and interpret cybervetting practices.

Data Validity and Trustworthiness

To enhance the trustworthiness and credibility of the analysis, multiple strategies were employed in line with established qualitative research guidelines.

Peer Debriefing

Peer debriefing was used to strengthen the credibility of the analysis. As described by Lincoln and Guba (1985), peer debriefing involves engaging a knowledgeable individual to critically examine the researcher's interpretations. Throughout the coding and interpretation process, data excerpts, developing codes, and emerging interpretations were shared with a colleague familiar with qualitative methods but not directly involved in the study. This peer challenged assumptions, offered alternative perspectives, and questioned conclusions that may have been influenced by the researcher's positionality.

This process served as a form of analytical accountability, helping to reduce bias and ensuring that the findings remained grounded in participants' accounts rather than researcher

expectations (Creswell & Poth, 2018). By making the analytic process more transparent and reflexive, peer debriefing enhanced the overall credibility of the study.

Thick Description

Thick description was employed to provide rich, contextualized representations of participants' experiences. According to Lincoln and Guba (1985), thick description enables readers to assess the transferability of qualitative findings to other contexts. In this study, detailed descriptions, illustrative quotations, and careful attention to social and cultural context were used to present participants' perspectives in a way that reflects not only what they said but also how they understood and conveyed their experiences.

This approach aligns with Tracy (2020)'s criteria for qualitative rigor by allowing the complexity of participants' viewpoints to be fully represented. Together, these strategies enhanced the credibility, transparency, and overall trustworthiness of the study.

Positionality Statement

Before moving to the United States for my studies, I had lived and worked exclusively in Nigeria. In that context, the idea of employers reviewing an individual's social media presence as part of hiring or promotion decisions was unfamiliar. While I was aware of conventional background checks, such as verifying criminal records, the practice of cybervetting was not something I had encountered or critically considered. My awareness of this practice only developed after engaging with it in an academic setting in the United States.

Coming from a cultural context that emphasizes community, interpersonal relationships, and respect for authority, I may have initially been more inclined to accept practices that appear to serve organizational interests, even when they raise concerns about individual privacy. However, exposure to perspectives that prioritize personal autonomy and privacy has heightened

my sensitivity to the ethical implications of cybervetting. Navigating these differing cultural frameworks has encouraged a more critical and reflective approach to the issue.

This dual perspective shapes my approach as a researcher. It allows me to draw on my cultural background while maintaining enough analytical distance to question assumptions that may otherwise go unexamined. At the same time, this understanding of cultural context is useful in interpreting the perspectives participants express, although it also introduces limitations. It may create the assumption that I fully understand participants' accounts when, in reality, their meanings are best understood through their own words. I therefore remain attentive to participants' direct explanations, ensuring that my interpretations are grounded in what is explicitly articulated rather than shaped solely by my prior assumptions, as someone familiar with the culture.

It is also worth noting that, as a male researcher, my initial recruitment relied primarily on contacts within my social network, which is predominantly male. This may have introduced selection bias, as these participants tended to refer other male participants from their own networks. Being aware of the potential impact of this bias on the diversity of responses, I took additional steps to address it. Even after reaching data saturation, I intentionally recruited more female participants, bringing the total number of participants to 14 in order to improve gender diversity within the sample.

Chapter 4 - Findings

This chapter presents findings from 14 interviews of Nigeria employees. The interviews sought to understand how these Nigeria employees perceive cybervetting, particularly regarding issues of privacy and fairness; the factors shaping their perception; and how specific cultural dimensions and values, such as collectivism, power distance, and uncertainty avoidance, shape their perceptions.

As discussed in the previous chapter, the participants, all assigned pseudonyms to protect their identities, were drawn from a range of professional backgrounds, including banking, finance, technology, agriculture, and fashion. The sample comprised both male and female participants, although males were more predominant (11 out of 14 participants). Most participants were between their mid-20s and early 40s. All were well-educated, with several holding advanced degrees, indicating a relatively high level of professional and academic exposure across the group. Participant characteristics are summarized in Table 1.

The findings are organized according to the study's research questions. The first section addresses RQ1, examining how employees in Nigeria perceive cybervetting, particularly in relation to issues of privacy and fairness. Three key themes emerged from the data. First, participants described cybervetting as extending organizational control beyond workplace boundaries, raising concerns about privacy and personal autonomy. Second, participants expressed uncertainty regarding how online information is interpreted, highlighting the potential for misjudgment and loss of context. Third, participants revealed a range of negotiated responses, reflecting varying degrees of acceptance and resistance to cybervetting practices across different contexts.

The second research question focuses on the factors influencing these perceptions. The analysis identifies four key dynamics. Employees' economic positioning shapes how freely privacy concerns are expressed, with job security influencing willingness to resist or accept surveillance practices. Institutional normalization of data access further conditions acceptance, as widespread digital monitoring practices render cybervetting more familiar and, in some cases, expected. Transparency emerges as a critical threshold for perceived legitimacy, with participants placing importance on openness regarding how information is accessed and used. Finally, moral framings of responsibility serve to normalize cybervetting practices.

The final section shifts to present findings for how specific cultural dimensions values, such as collectivism, power distance, and uncertainty avoidance, shape these feelings of cybervetting.

RQ1.How do employees in Nigeria perceive Cybervetting, particularly regarding issues of privacy and fairness?

Cybervetting Extends Organizational Control Beyond Workplace Boundaries

Cybervetting operates as a mechanism that extends organizational control beyond formal workplace boundaries into employees' personal digital spaces. At its core, this process redefines the scope of employer authority by collapsing the distinction between personal and professional domains. Rather than treating social media as a separate sphere of personal expression, cybervetting reconstitutes it as a site of professional evaluation. This shift expands what counts as legitimate organizational oversight, bringing previously non-work-related behaviors under employer scrutiny. In doing so, cybervetting disrupts individuals' ability to manage privacy across contexts and, in some cases, facilitates ongoing forms of monitoring that extend beyond the workplace.

Collapse of Personal–Professional Boundaries

Cybervetting collapses the boundary between personal and professional life by redefining personal digital spaces as professionally relevant. Participants consistently positioned social media as an extension of private life—a domain governed by norms of personal interaction, leisure, and self-expression. As Kay, a young professional working in real estate, notes, "outside of work, I have my personal life. And social media is like an extension of that... I feel like it's personal to me, not part of my work." However, employer access to these spaces reconfigures them as evaluative environments, thereby expanding the criteria through which individuals are judged in professional contexts.

Tee, a banker, asserted that "there should be no mixing of both," which further underscores this expectation of domain separation. This distinction reflects an underlying expectation that personal and professional domains are governed by different norms of evaluation. Cybervetting disrupts this separation by introducing professional scrutiny into spaces not structured for that purpose. As a result, behaviors previously understood as belonging to the personal sphere are brought into professional consideration. Rather than remaining separate, these domains become blurred, with social media spaces no longer clearly defined as either personal or professional. The rejection of cybervetting, therefore, reflects resistance to this erosion of boundaries and the intrusion of professional oversight into areas participants perceive as private.

Kev highlighted the structural inconsistency this produces: "If you're saying work is work and personal life is personal life, why are you now going into my social media?" Here, cybervetting exposes a contradiction within organizational logic: while employees are expected to compartmentalize personal and professional identities, employers simultaneously collapse

these boundaries through digital access. In doing so, cybervetting extends organizational authority into domains previously considered outside its legitimate scope.

Disruption of Contextual Privacy

Cybervetting disrupts privacy not by exposing hidden information, but by reassigning personal content to unintended audiences. Participants consistently framed privacy not as secrecy, but as the ability to control who their content is for. As Kev puts it, “(my) social media is public doesn’t mean it’s all should have access or is permitted.” In this sense, privacy is defined by audience alignment rather than visibility. Cybervetting violates this alignment by positioning employers as legitimate viewers and interpreters of content that participants produce for personal, non-professional audiences, thereby constituting a form of privacy intrusion even in ostensibly public spaces.

Kay’s statement made this distinction particularly clear: “Outside of work, I have my own personal life... I feel like it’s (social media) personal to me, not part of my work.” This fundamentally reflects an expectation about the audience. By defining social media as “personal,” Kay is not simply marking it as private, but specifying that it is intended for a particular set of viewers—friends, peers, and social contacts—not employers. The issue, therefore, is not that employers can see the content, but that they are not the intended audience for it. By inserting employers into spaces where they are not socially recognized as legitimate observers, cybervetting disrupts this expectation of privacy even within public settings. Privacy, in this sense, is compromised.

This logic is further reinforced by Hammie’s account:

Just because things are available online doesn’t mean I want my employers seeing them... I don’t. I know my social media is public, yes. But my employers are not the people I want

to necessarily see those things... it just feels like an invasion... like they're entering my space without permission.

Hammie's description explicitly frames cybervetting as an invasion, despite the public nature of the content. His analogy illustrates that even in open environments, individuals maintain expectations about appropriate audiences. The presence of an unintended observer—particularly one with evaluative power—transforms the experience of visibility into one of intrusion. Cybervetting, therefore, collapses the distinction between who can see and who should see, undermining individuals' ability to regulate their self-presentation.

Extension into Surveillance

Cybervetting is experienced by participants as introducing a condition of surveillance, where employer access to social media renders their personal digital activity subject to constant observation. Rather than being understood solely as a discrete, episodic evaluative practice, there is a sense in which it becomes embedded as an ongoing presence, placing individuals within the scope of organizational monitoring and extending the feeling of being observed beyond formal workplace settings.

At a former job, Lee revealed that she was being constantly monitored through her social media, to the point she felt "it was a witch-hunt." She recounted feeling "watched" all the time—"it wasn't just about work anymore," she said. What began as "innocently" dropping her social media account became a channel through which her bosses monitored her whereabouts. This shift reflects how cybervetting moves from a one-time act of evaluation into a sustained mode of observation, where personal visibility becomes continuous rather than situational.

Lee's experience signals a broader transformation in how cybervetting is understood—not simply as checking, but as a condition that extends into the routine of everyday life. The sense of

“being watched” reflects an awareness that personal activity is no longer fully outside the reach of employer visibility, blurring the boundary between organizational oversight and personal space.

Zay and Zoe also shared that they had encountered situations where bosses directly engaged with their online activity, including posts they had liked or commented on. In particular, Zoe noted that her boss’s repeated engagement with her online behavior reinforced this perception: “It just made me too conscious... like someone was looking over [my] shoulder all the time.” This metaphor does more than describe observation—it captures how the *possibility* of being watched becomes internalized, shaping how individuals experience their online presence.

This reflects a form of surveillance that operates not only through direct monitoring, but through the awareness that monitoring can occur at any time. Participants may not be monitored at all times, but the possibility that they could be creates a constant feeling of being watched. In this way, cybervetting functions in a manner similar to a “Big Brother” dynamic, where the power of surveillance lies not only in actual observation, but in the constant possibility of it.

As Tee puts it, employers “just really need to let people breathe,” highlighting how this perceived surveillance is experienced as excessive and intrusive. Together, these accounts underscore how cybervetting is interpreted not simply as an evaluative tool, but as a form of surveillance that reshapes how individuals experience autonomy, visibility, and control in their personal lives.

Cybervetting Produces Interpretive Uncertainty and Risk of Misjudgment

Cybervetting produces interpretive uncertainty by requiring employers to make judgments based on fragmented and contextually detached information. Participants consistently expressed concern that social media content, when removed from its original context, becomes open to misinterpretation. Rather than providing an accurate representation of individuals’

character or professional suitability, cybervetting was understood as introducing ambiguity, where meaning is unstable and subject to incorrect inference. In this sense, the practice does not simply reveal information, but reshapes it in ways that increase the likelihood of misjudgment.

Collapse of Contexts

Cybervetting collapses context by detaching social media content from the conditions under which it was originally produced and understood. Participants emphasized that online expressions are often shaped by specific social, cultural, and situational factors that are not visible to external observers. When employers interpret such content without access to these contextual cues, meaning becomes distorted.

Tee expressed concern about being “judged based on anything” found on his social media, a space he does not associate with professional evaluation. He acknowledged that his profile contains “silly” and “casual” posts, which he uses to relax and enjoy his “me time.” However, these forms of expression are produced within a personal context and are not intended to represent his professional identity. When such content is assessed without understanding its original context, it becomes vulnerable to misinterpretation. In this way, cybervetting risks stripping posts of their situational meaning, leading to judgments that do not accurately reflect the individual’s character or suitability in a professional context. Eyo further illustrated how “people can take things out of context,” noting that posts made in response to specific situations may be interpreted “completely differently” when removed from their original circumstances.

Drawing on his experience at a multinational company, Eyo recounted learning from a friend in the HR department that recruiters look for “safety behavioral pattern[s]” to infer temperament or character. He questioned the validity of such assessments, emphasizing that the absence of context makes accurate interpretation difficult:

It's easy to misunderstand people from social media. For example, during the EndSARS protests, someone who maybe lost a relative might post something angry about the police. But if you just see that post without context, you might think the person is violent or aggressive. That's not the full picture. It's hard to really know someone from one tweet or one comment.

This highlights how meaning is not inherent in the content itself, but dependent on shared context between the speaker and their intended audience. Cybervetting disrupts this relationship by introducing an external observer who lacks the contextual knowledge necessary to interpret the content accurately. And so, the evaluation due is not always taking into account the situations to make a full and complete judgement.

As a result, behaviors that are socially intelligible within one context may be misread when evaluated through a professional lens. Participants described how humor, cultural references, or situational expressions could be taken literally or judged negatively when stripped of their original meaning. Cybervetting, therefore, does more than not simply access information; it repositions information within a different interpretive frame, where the risk of misunderstanding is significantly increased.

In this way, the collapse of context produces interpretive uncertainty, as employers are required to make evaluative decisions based on incomplete or decontextualized information. The concern is not only that content is visible, but that it is vulnerable to misreading when removed from the conditions that give it meaning.

Fixing Identity Across Time

In addition to collapsing context, cybervetting was perceived as fixing identity across time, ignoring the evolving nature of individuals' beliefs, behaviors, and self-presentation. Participants

expressed concern that past content, often created under different circumstances, could be used to make present judgments, without consideration for personal growth or change.

Hammie reflected this concern:

People change. There are things I posted years ago, maybe when I was in school and not really thinking about jobs or anything serious. But those things are still there. Someone can go and dig them up... you know things don't really disappear from the internet. It just feels unfair to judge someone now based on things that don't represent who they are anymore

This highlights how cybervetting constructs identity as static, where past expressions are treated as enduring indicators of character. Rather than accounting for change over time, the practice allows historical content to be reintroduced into present evaluation, effectively freezing individuals within earlier versions of themselves.

Grand similarly noted that people evolve:

Posts from like five years ago, when I was younger and just starting out, don't reflect who I am professionally today. Using those kinds of posts to judge me now isn't accurate at all. That's not who I am anymore.

These accounts suggest that cybervetting disregards the temporal dimension of identity, treating digital traces as fixed and continuously relevant. This creates a risk of misjudgment, where individuals are evaluated based on outdated or no longer representative information.

By collapsing temporal boundaries, cybervetting transforms past behavior into present evidence, without accounting for shifts in perspective, maturity, or context. In doing so, it reinforces a simplified and static representation of identity, increasing the likelihood that individuals will be judged inaccurately.

Employees Actively Negotiate Legitimacy of Cybervetting Across Contexts

Employees actively negotiate the legitimacy of cybervetting across contexts, rather than interpreting it as uniformly acceptable or unacceptable. Analysis of the interview data indicates that participants evaluate cybervetting by applying context-specific criteria, assessing when, how, and under what conditions it is justified. Legitimacy, in this sense, is not treated as an inherent property of the practice, but as something constructed through ongoing evaluation of competing considerations.

Rather than expressing clear support or opposition, participants occupied ambivalent positions, simultaneously recognizing the perceived utility of cybervetting while questioning its fairness and scope. This suggests that legitimacy is not inherent to the practice itself, but is actively assessed and recalibrated in relation to specific contexts.

One of the primary criteria participants used in this evaluation was platform type. Participants consistently distinguished between professional and personal social media spaces, using this distinction to determine whether employer scrutiny was appropriate. Professional platforms were constructed as legitimate sites of evaluation, while personal platforms were positioned as outside the acceptable scope of employer access. Lee's account illustrated this boundary: "Yes, definitely. LinkedIn is fine... it makes sense for employers to check that. That's what it's for."

Here, legitimacy is tied to the intended function of the platform. Because LinkedIn is designed for professional self-presentation, employer access is perceived as appropriate. In contrast, platforms such as Instagram, Facebook, and TikTok were framed as personal domains oriented toward social interaction and self-expression. Applying professional evaluation to these

spaces was therefore interpreted as a misalignment of purpose, rendering cybervetting inappropriate in those contexts.

A similar evaluative process emerges in relation to job relevance. Participants assessed legitimacy based on whether a meaningful connection existed between online behavior and job responsibilities. Sunny articulated this conditional logic by stating, “It really depends on the kind of job...”

This reflects a pattern in which cybervetting is considered more acceptable when participants perceive a clear link between personal conduct and professional expectations. Without such a connection, the practice is viewed as unnecessary and unjustified.

Kay reinforced this boundary by stating, “I think it should only apply if the job actually involves social media...” Zoe similarly questioned the relevance of cybervetting in unrelated professions:

If the job is something like social media manager or content creator, then fine, it makes sense. But if it’s something like a doctor or an accountant, then why are you even asking for it? What’s the connection?

In addition to platform type and job relevance, participants also emphasized transparency as a key factor shaping the perceived legitimacy of cybervetting practices. Acceptance was more likely when employers were open about whether and how they engaged in cybervetting, including clearly communicating the scope, purpose, and criteria of evaluation. Participants’ accounts suggest that the absence of transparency introduces a sense of opacity that undermines trust and reconfigures otherwise acceptable practices as intrusive. As Sel noted, “I don’t have a problem with them checking, but the way it’s done sometimes... it just feels like it’s happening in the dark,” highlighting how undisclosed processes generate discomfort even when the practice itself is not

outright rejected. Similarly, Kuni framed the issue not as opposition to cybervetting per se, but to its execution. She stated, “I just have a problem with how they go about it. It feels like it’s done behind your back.”

These concerns were further reinforced by participants’ experiences during hiring processes, where requests for social media information were often embedded within application materials without clear explanation. A recurring pattern across accounts was that social media handles were requested during application processes without any explicit clarification of how the information would be used. In most cases, this request appeared as part of a form, accompanied by little or no contextual detail, leaving applicants to infer its purpose. Ike reflected on this ambiguity: “I mean, we could guess what they wanted it for, obviously... but it wasn’t clearly stated. They didn’t really explain anything.”

As a whole, these accounts indicate that transparency functions as a threshold condition for legitimacy. While it does not necessarily resolve all concerns, it shapes whether cybervetting is interpreted as procedurally fair or covertly invasive.

Across these accounts, participants do not evaluate cybervetting in absolute terms, but through structured, context-dependent judgments about appropriateness. Platform type, job role, perceived relevance, and transparency function as criteria through which legitimacy is actively negotiated. Cybervetting, therefore, is understood not as inherently acceptable or unacceptable, but as a practice whose legitimacy is contingent, constructed, and continuously reassessed.

RQ2: What factors influence employees’ perceptions of cybervetting practices?

Beyond examining how employees perceive cybervetting, this study also sought to identify the factors that shape these perceptions. Analysis of the interview data indicates that

employees' acceptance or rejection of cybervetting is not solely based on the practice itself, but is influenced by a set of underlying conditions that structure how it is interpreted and evaluated. Rather than holding fixed or uniform positions, participants' views were shaped by broader economic, institutional, and normative considerations that inform their judgments about legitimacy, fairness, and necessity.

The findings suggest that employees interpret cybervetting within a wider context of constraints and expectations, rather than as an isolated organizational practice. In this sense, perceptions are produced through the interaction of multiple factors that shape both evaluative judgments and behavioral responses.

Three key factors emerged from the data: economic positioning conditions the expression of privacy beliefs; institutional normalization of data access shapes acceptance of cybervetting; and moral framing of responsibility influences how the practice is justified. Together, these factors indicate that employees' perceptions of cybervetting are structured by broader social and organizational forces that extend beyond the practice itself.

Economic Positioning Conditions the Expression of Privacy Beliefs

Economic positioning emerged as a key factor shaping how employees interpret and respond to cybervetting practices. Participants' accounts indicate that acceptance of cybervetting is not solely determined by personal beliefs about privacy or fairness, but is significantly conditioned by individuals' economic circumstances and perceived job security. In this sense, economic positioning does not simply influence attitudes toward cybervetting, but structures the extent to which employees are able to act on those attitudes.

Across interviews, participants frequently expressed concerns about privacy, fairness, and the intrusiveness of cybervetting. However, these concerns did not always translate into

resistance. Instead, a tension between personal beliefs and the practical need to secure or maintain employment was consistently evident. This suggests that acceptance of cybervetting often reflects constrained choice rather than genuine endorsement.

Lee illustrated how economic positioning can enable resistance:

That one is a deal breaker for me. I won't drop my social media handle for any job.

Now, I can say no. It's easier for me to take that stand because I'm in a better place financially. But back then? I wouldn't have even thought twice. I would have just given it. At that time, getting the job was the priority. Honestly, if it was before, with how things were, I would have overlooked my concerns. You just need the job. So, you don't really have the luxury to start arguing about privacy or anything like that.

Her account makes explicit the role of economic stability in shaping the capacity to resist. While she is now able to reject cybervetting practices, she acknowledges that under different financial conditions, compliance would have been unavoidable. This highlights how resistance is not purely a matter of principle, but is contingent on one's economic position.

This position was not widely shared across participants. Others described being less able to take such a stance, emphasizing the risks associated with non-compliance. As Hammie noted, "unfortunately, if you don't comply, you won't get the job." This reflects a broader recognition that economic constraints compel individuals to accept practices they might otherwise reject. Unlike Lee, who describes being in a more stable financial situation and able to uphold her privacy preferences, many participants framed compliance as necessary within the realities of the labor market.

As another participant, Moe, explained, declining such requests could “jeopardize employment opportunities,” making compliance a pragmatic choice rather than a voluntary one. In this context, cybervetting is not simply accepted, but navigated under conditions where refusal carries significant economic risk. Interestingly, even some participants who had earlier expressed support for cybervetting revealed hesitation when asked about their personal willingness to comply. For instance, Sunny, who had initially described cybervetting as reasonable, responded differently when asked if he would voluntarily provide his social media handles. “No... I don’t think I would,” he said. When asked to elaborate, he hesitated and then added: “I just... I’d rather not. It’s not like I’m doing anything bad online or anything like that. I just don’t feel comfortable with it.”

Similarly, Ike, who argued that individuals with “no cockroach in their cupboard” should not fear cybervetting, also admitted that, if given a choice, he would prefer not to disclose his social media accounts. These responses suggest that expressed support for cybervetting does not always translate into genuine personal acceptance. Instead, they point to a form of pragmatic compliance, where individuals outwardly justify or accept the practice while internally maintaining reservations.

This tension between belief and behavior highlights the extent to which cybervetting is often accepted not because it is perceived as fair, but because it is seen as unavoidable within the current labor market.

This dynamic reveals a clear distinction between expressed beliefs and enacted behavior. While participants may view cybervetting as invasive or unfair, their responses are shaped by the practical demands of securing employment. Economic positioning, therefore, mediates how

privacy concerns are translated into action, determining whether individuals are able to resist or are compelled to comply.

Institutional Normalization of Data Access as a Structural Factor

Institutional normalization of data access operates as a structural factor shaping how cybervetting is interpreted and evaluated. Participants' accounts indicate that cybervetting is not understood as an isolated organizational practice, but as part of a broader landscape in which institutions increasingly claim access to individuals' personal and digital information. In this context, employees' responses to cybervetting are shaped by their positioning within an environment where data extraction is already embedded in routine institutional processes. Kev's illustrated this broader structural pattern: "Privacy is a fundamental right... but look at how even banks are now asking for your social media handles... all in the name of security or fraud prevention."

Rather than simply expressing concern about privacy, Kev situated cybervetting within a wider institutional logic in which access to personal data is justified through narratives of necessity, such as security and fraud prevention. His reference to banking practices indicates that employer requests for social media access are interpreted as part of an expanding system of institutional data collection, rather than as a singular or exceptional demand.

This broader pattern is further reflected in participants' accounts of other institutional practices. Tee, for instance, described previous workplace requirements involving extensive personal documentation, including identity verification processes that extended beyond basic employment needs. Similarly, Moe pointed to regulatory practices such as biometric data capture for SIM card registration, where individuals are required to submit personal information as a condition for access to essential services.

These examples indicate that cybervetting operates within a wider ecosystem of institutional data access. The proliferation of such practices establishes a structural context in which requests for personal information are normalized across multiple domains. Within this environment, employer access to social media is not encountered as an entirely new or distinct form of intrusion, but as consistent with existing patterns of institutional behavior.

As a result, employees' perceptions of cybervetting are shaped by this broader structural condition. The normalization of data access across institutions reduces the perceived exceptionalism of cybervetting, influencing how it is interpreted and responded to. In this sense, acceptance is not simply a reflection of individual attitudes toward cybervetting itself, but is produced within a system where organizational access to personal information is already an established and expected practice.

Moral Framing of Responsibility as a Factor Shaping Acceptance

Moral framing of responsibility functions as a key factor shaping how some employees interpret and justify cybervetting practices. Participants' accounts indicate that acceptance of cybervetting is, in part, grounded in a moral logic that positions individuals as responsible for the content they share online. Within this framing, cybervetting is interpreted as legitimate on the assumption that individuals who have acted appropriately have nothing to fear from scrutiny.

Ike's captures this perspective: "If you don't have cockroach in your cupboard, you shouldn't be scared." This statement reflects a moral framing in which transparency is equated with innocence, and concern about cybervetting is implicitly associated with wrongdoing. Under this logic, the burden shifts to individuals to ensure that their online presence is beyond reproach. Cybervetting, therefore, is not seen as inherently intrusive, but as a reasonable practice that simply reveals what is already there.

This logic is further reinforced in Kuni's account, where cybervetting is framed as a way to confirm moral character: "So they can know that the person is a good person and has a good character." Here, cybervetting is positioned as a tool for verifying integrity, suggesting that personal character can and should be assessed through available digital traces. This extends the moral expectation that individuals are accountable not only for their actions, but for how those actions are publicly represented and interpreted.

Sunny similarly alludes to this expectation, emphasizing that claims about one's character should not be taken at face value: "Your boss shouldn't just take your word for it that you are a good person." This reflects a broader belief that personal assertions are insufficient, and that verification is necessary. Within this framing, cybervetting becomes justified as a means of validating character, rather than an overreach into personal life.

Taken together, these accounts illustrate a consistent moral logic in which cybervetting is normalized through the expectation that individuals should be able to withstand scrutiny. Responsibility is placed on employees to maintain a digital presence that reflects positively on their character, and organizational access is justified as a way of confirming this alignment. In this sense, cybervetting is interpreted not simply as an organizational practice, but as a legitimate response to individual conduct.

At the same time, this framing subtly encourages individuals to be mindful of how they present themselves online, as their digital activity is understood to carry evaluative consequences. In this way, moral framing shapes acceptance by positioning cybervetting as a reflection of personal responsibility rather than institutional overreach.

RQ3: How do cultural dimensions or values, such as collectivism, power distance, and uncertainty avoidance, shape the interpretation of cybervetting?

The final research question examined how cultural dimensions shape employees' interpretations of cybervetting practices. Drawing on existing literature, cultural dimensions such as collectivist orientation, power distance, and uncertainty avoidance and respond to privacy concerns and organizational surveillance practices, including cybervetting. Hence, these dimensions were used as analytical lenses to explore how participants make sense of cybervetting within their specific cultural context.

Analysis of the data reveals how these cultural dimensions shape interpretation in distinct ways. A collectivist orientation functions as a basis for legitimizing cybervetting, particularly when the practice is framed in relation to collective interests or organizational reputation. In contrast, power distance reveals limits to legitimacy, as participants' recognition of hierarchical authority does not necessarily translate into acceptance of employer intrusion. Finally, uncertainty avoidance operates in a more nuanced manner: while participants show a generally moderate orientation toward uncertainty in everyday contexts, they nonetheless express resistance that emerged not from ambiguity itself, but from how that ambiguity translated into practice, especially when outcomes were perceived as intrusive or misaligned with expectations of privacy and fairness.

Collectivist Orientation as a Basis for Legitimizing Cybervetting

A collectivist orientation functions as a basis through which cybervetting is interpreted as legitimate, particularly when it is framed in relation to collective interests such as organizational reputation, social responsibility, and group representation. Participants' accounts indicate that, within this orientation, the evaluation of cybervetting extends beyond individual privacy

concerns to include its perceived value for the broader group. In this sense, acceptance is shaped by a prioritization of collective outcomes over individual autonomy.

Across interviews, participants with stronger collectivist orientations framed their online behavior as inherently tied to their affiliations with family, community, and organization. Within this logic, personal conduct is not viewed as entirely private, but as reflective of the groups to which individuals belong. This framing provides a basis for legitimizing employer scrutiny, as cybervetting is interpreted as a means of ensuring alignment with shared values.

Sunny's explain this orientation:

I come from a well-cultured family... so I'm always cautious about what I share online. I'm very conscious of representing both myself and my organization. I avoid posting things that could reflect negatively on the company... My bosses have a right, I think, to make sure I reflect the kind of values they want and not being a dent to their image. I am a part of the organization and a representative of them.

Here, cybervetting is justified through a logic of representation, where individual behavior is understood as having implications for the collective. The emphasis on being “a representative” of the organization reframes employer access as a legitimate means of protecting group identity and reputation.

Ike similarly expresses acceptance grounded in a sense of obligation to the organization. He declared, “I see myself as a good rep for the company... I feel a sense of responsibility to the company, so it's okay for them to check.” This reflects a moral alignment between personal conduct and organizational expectations, where scrutiny is accepted as a reasonable extension of one's responsibility to the group. Under this framing, cybervetting is not experienced as

intrusive, but as consistent with the expectation that individuals should uphold standards that reflect positively on their affiliations.

Kuni reinforces this collectivist logic by framing cybervetting as a form of character verification undertaken in the interest of protecting the group:

“This is about character verification... because of the image of the company.

Getting to know people beyond what they have submitted on their CV. If I were a boss, I would also do it to be sure that I uphold the image of the company.”

Here, cybervetting is not positioned merely as an evaluative tool, but as a mechanism for safeguarding collective identity. The emphasis on “upholding the image of the company” reflects a concern with how individual behavior reflects on the group as a whole. Within this framing, assessing personal conduct becomes a way of ensuring that individuals align with shared values and do not undermine collective reputation. Cybervetting, therefore, is interpreted as a legitimate practice insofar as it serves the interests of the group, reinforcing the expectation that individuals bear responsibility for maintaining the integrity of their organizational affiliations.

In contrast, this collectivist grounding for accepting cybervetting did not resonate with participants such as Kay, who did not perceive herself as representing any broader social or organizational group. As she explained, she did not “feel particularly representative of any community” and did not “think much about familial ties when it comes to how [she] represents [herself] online.” This detachment from collective identity shapes how cybervetting is interpreted, as the absence of a representational obligation reduces the perceived legitimacy of employer scrutiny.

From the data, collectivist orientation functions as a central basis through which cybervetting is legitimized, by positioning individual behavior as accountable to the group.

When individuals see themselves as representatives of their organization, family, or community, personal conduct is understood as socially consequential rather than purely private. Within this logic, employer scrutiny is reframed as a means of protecting collective identity and ensuring alignment with shared values. In contrast, where this sense of representation is absent, the legitimacy of cybervetting is more readily questioned. Collectivist orientation, therefore, shapes both the acceptance and justification of cybervetting by grounding it in responsibility to the group rather than individual autonomy.

Power Distance and the Limits of Cybervetting Legitimacy

Analysis of the interview data indicates that while high power distance is evident in participants' social and workplace interactions, it does not play a significant role in shaping their acceptance of cybervetting practices. This finding contrasts with existing literature, which often suggests that deference to authority in high power distance contexts leads to greater acceptance of organizational practices such as cybervetting.

Participants' accounts consistently reflect patterns of deference toward authority figures, particularly within workplace environments. Supervisors were described as holding significant power and being treated with a high level of respect, reinforcing hierarchical relationships. For example, Sunny described situations where communication with supervisors is often one-sided, noting that messages may go unanswered without being questioned. Similarly, Moe explained that bosses "yield power" in ways that reinforce clear status distinctions between employees and management. These interactions point to workplace dynamics in which authority is recognized and rarely challenged.

This orientation toward deference is further shaped by broader cultural norms. In the Nigerian context, respect for elders is deeply embedded, and this often extends into

organizational settings. Participants noted that it is common to refer to older individuals in parental terms, and some supervisors expect similar forms of address from junior staff. Tee, for instance, described resisting this expectation, stating that “only my actual parents get the title of mum and dad.” He further explained that even professional forms of address could be frowned upon, noting that “you can’t say Mr. Luke, for example because he would be angry, and expects you to refer to him as sir.”

These accounts clearly reveal the presence of high power distance, reflected in both workplace interactions and broader social practices. However, this cultural orientation toward deference does not translate into acceptance of cybervetting practices. Participants consistently distinguished between respecting authority and agreeing with how that authority is exercised. Even individuals who appeared comfortable with hierarchical norms did not necessarily support cybervetting practices. For instance, Grant, who described referring to his boss as “dad,” did not express acceptance of cybervetting based on this deference.

This finding suggests that deference to authority and responses to cybervetting operate as distinct processes. While power distance shapes how individuals relate to authority, it does not determine whether they accept cybervetting practices. In this sense, high power distance coexists with critical evaluation, rather than producing automatic acceptance of employer intrusion into personal digital lives.

Uncertainty Avoidance and Resistance to Cybervetting Ambiguity

From the interview data, resistance to cybervetting appears not to stem from an inherent intolerance for uncertainty, but rather from how cybervetting practices are experienced over time. Participants’ accounts indicate a pattern consistent with moderate uncertainty avoidance, rather than a clearly high or low cultural orientation. From their narrations, participants indicated

a relative tolerance for ambiguity, particularly during the initial stage of providing social media information. Many reported submitting their handles without questioning how the data would be used, suggesting an initial acceptance of unclear or unspecified procedures. Kine explained, “I just filled out a form of our social media account, and was told what they were going to do with it,” indicating a willingness to comply despite limited clarity. Similarly, others also reported submitting their social media handles without questioning how the information would be used.

Zoe explained, “at the point when I applied for the job, the last information to provide was social media handles.” When asked if it disturbed her not knowing how the process of social media screening would go, she said, “No, not really.”

Lee noted that she “did not think much” about the form at the time of completion, only reflecting on its implications after observing how her social media content was later engaged. Similar accounts were shared by other participants, who described providing such information without explicit explanation, reinforcing a pattern of early-stage ambiguity tolerance.

However, this tolerance was not unconditional. As the context and consequences of cybervetting became more visible, participants’ evaluations shifted. Importantly, the initial lack of clarity surrounding cybervetting practices did not, in itself, constitute a primary concern. Instead, resistance emerged when these practices were perceived to infringe on personal privacy or exceed acceptable boundaries. In this regard, ambiguity was initially accommodated, but it became problematic when it resulted in outcomes interpreted as intrusive or misaligned with participants’ expectations.

This progression reflects a context-dependent engagement with uncertainty, characteristic of moderate uncertainty avoidance. Rather than exhibiting a strong preference for strict rules (as in high uncertainty avoidance) or a broad acceptance of ambiguity (as in low uncertainty

avoidance), participants appeared to tolerate uncertainty provisionally and reassess it based on unfolding experience. Their responses suggest that the legitimacy of cybervetting was not judged solely on the presence or absence of uncertainty, but on how that uncertainty translated into practice— particularly in relation to perceived fairness, relevance, and respect for personal boundaries.

Taken together, these findings indicate that resistance to cybervetting was not primarily driven by ambiguity itself, but by participants' retrospective evaluation of how ambiguous processes were enacted. This supports an interpretation of moderate uncertainty avoidance in which uncertainty is tolerated at the outset but remains subject to revision when it produces outcomes that conflict with socially and personally defined limits. In this sense, participants' calls for greater transparency reflect not a discomfort with uncertainty, but a reaction to perceived boundary violations and the erosion of contextual privacy.

Chapter Summary

This chapter presented findings from interviews with Nigerian employees on their perceptions of cybervetting. Overall, cybervetting was viewed as extending organizational control into personal digital spaces, raising concerns about privacy, fairness, and blurred personal–professional boundaries, while also introducing risks of misinterpretation due to lack of context. Participants did not respond uniformly but instead evaluated the legitimacy of cybervetting based on factors such as platform type, job relevance, and transparency. Their responses were further shaped by broader conditions, including economic constraints, the normalization of institutional data access, and moral beliefs about personal responsibility. Cultural dimensions also played a role: collectivism supported acceptance when cybervetting was linked to group interests, power distance did not necessarily translate into acceptance, and

uncertainty avoidance emerged as context-dependent, with participants initially tolerating ambiguity but later resisting when outcomes were perceived as intrusive or unfair.

Chapter 5 - Discussion

This study examined how Nigerian employees perceive cybervetting, with particular attention to issues of privacy and fairness, the factors shaping these perceptions, and the role of cultural values such as collectivism, power distance, and uncertainty avoidance in interpreting the practice. The findings show that participants did not view cybervetting in simple terms as either wholly acceptable or wholly unacceptable. Instead, their responses reflected a complex and negotiated process in which cybervetting was evaluated according to contextual expectations, perceived relevance, transparency, and the broader social and economic conditions within which employment decisions are made.

In this chapter, these findings are discussed in relation to the existing literature and the study's theoretical framework. Specifically, the discussion reveals how the findings both support and extend Geert Hofstede's cultural dimensions theory by showing that employees' interpretations and reactions to cybervetting are shaped not only by cultural values, but also by contextual and structural factors that are not fully accounted for within the theory. In addition to its theoretical contributions, this chapter outlines the practical implications of the study, followed by a discussion of its limitations and recommendations for future research.

Theoretical Contributions

This study makes three interrelated theoretical contributions, each developed through one of the following findings. First, it extends Communication Privacy Management and contextual integrity theory by showing that audience-based privacy reasoning operates beyond the Western, individualistic contexts in which it has been primarily theorized. Second, it extends surveillance scholarship by situating workplace cybervetting within a broader institutional ecology of state-mandated data regimes, drawing attention to how centralized identity infrastructures in the

Global South pre-condition citizens to workplace surveillance in ways that existing theorizing has underexamined. Third, it refines the application of cultural dimensions theory—particularly power distance—by revealing that cultural values function as interpretive resources rather than fixed predictors of behavior. Across these three contributions, the study introduces the concept of *pragmatic privacy compliance* to capture the gap between expressed acceptance and lived discomfort that characterized participants' accounts. Compliance, in this framework, is not the absence of critique but its accommodation under conditions that make open resistance impractical.

Cybervetting as a Dynamic and Contextually Negotiated Practice

The findings of this study show that employees' perceptions of cybervetting are best understood as a process of ongoing negotiation rather than a fixed position of acceptance or rejection. Across accounts, participants did not evaluate cybervetting in absolute terms. Instead, their responses reflected a context-dependent assessment shaped by perceived appropriateness, relevance, and the conditions under which the practice was enacted. Cybervetting was more acceptable when aligned with professional contexts or clearly justified, and more likely to be rejected when it extended into personal spaces or lacked explanation. As such, participants did not simply accept or reject cybervetting; they engaged in a contextual evaluation in which legitimacy was continuously reassessed.

However, a key pattern emerging from the data is the framing of cybervetting as a form of organizational control that extends beyond the workplace and disrupts established expectations of privacy. Participants consistently described social media as a personal domain, governed by norms of informal interaction and self-expression. Within this space, privacy was not understood as secrecy, but as control over appropriate audiences. The public visibility of

content did not imply that all audiences were legitimate viewers; rather, participants maintained clear expectations about who their content was intended for. When organizations fail to maintain this expectation through cybervetting, they disrupt what can be understood as participants' sense of "contextual privacy."

From this perspective, cybervetting was experienced as a privacy violation not because information was hidden, but because it was accessed and interpreted by an unintended audience—employers. In doing so, cybervetting collapses audience boundaries and repositions personal content within a professional evaluative context, reinforcing the idea that privacy violations can occur even in public spaces when contextual norms are breached (Nissenbaum, 2010; Petronio, 2002).

Structural Shaping of Cybervetting Perceptions

This study shows that employees' perceptions of cybervetting are shaped by underlying structural and contextual conditions that influence how the practice is interpreted and how individuals respond to it. Participants' evaluations do not emerge in isolation; rather, they are formed within an institutional environment where access to personal data is already normalized, routinized, and often unavoidable.

A particularly significant pattern is the normalization of institutional access to personal data as a structural condition shaping acceptance of cybervetting. Participants did not encounter cybervetting as an exceptional or novel practice, but as part of an established ecosystem in which institutions routinely collect, store, and circulate personal information.

The Nigerian context makes this structural condition especially visible. Systems such as the Bank Verification Number (BVN), National Identification Number (NIN), and mandatory SIM registration policies require individuals to surrender extensive personal and biometric data

as a condition for accessing basic services. SIM registration policies, for instance, link users' phone numbers directly to national identity databases, enabling traceability and institutional oversight (Nigerian Communications Commission, 2020). Similarly, the BVN system integrates millions of citizens into centralized identity infrastructures designed for continuous verification and monitoring (Central Bank of Nigeria, 2014).

In addition, recent regulatory developments further extend institutional access to personal data. The Central Bank of Nigeria has introduced customer due diligence guidelines requiring financial institutions to obtain customers' social media handles as part of Know Your Customer (KYC) processes (Central Bank of Nigeria, 2023). These are not isolated mechanisms, but interconnected systems that embed data extraction into everyday institutional interactions, reflecting what Lyon (2018) describes as the expansion of "surveillance societies," where monitoring becomes routine and normalized.

Within this environment, cybervetting is not experienced as a distinct intrusion but as a continuation of normalized institutional access to personal data. This normalization produces acceptance grounded in habituation rather than genuine approval. Individuals may recognize cybervetting as intrusive yet still comply because it aligns with broader expectations that access to personal information is a routine condition of institutional participation. In this way, normalization reduces resistance by rendering such practices familiar, necessary, and, in many cases, unavoidable. This pattern is consistent with research suggesting that repeated exposure to data collection practices can lead to diminished resistance and increased acceptance, even in the presence of privacy concerns (Acquisti, Brandimarte, & Loewenstein, 2015).

At the same time, this structural condition interacts with other factors that shape participants' responses. Economic positioning constrains the extent to which individuals can act

on their privacy concerns, often leading to compliance even in the presence of discomfort. Similarly, moral framings of responsibility reinforce acceptance by positioning individuals as accountable for their online presence, sustaining the belief that scrutiny is justified for those with “nothing to hide,” a logic widely documented in privacy research (Solove, 2011).

Taken together, these conditions give rise to what this study calls pragmatic privacy compliance, a pattern in which individuals outwardly accept or rationalize privacy-invasive practices due to economic pressures, normalized institutional access, and culturally embedded expectations, while internally maintaining contextually grounded reservations. Expressed acceptance in this framework cannot be read as endorsement; it often reflects the absence of viable alternatives rather than genuine approval.

Revisiting Power Distance: Authority, Legitimacy, and the Limits of Compliance

Another key insight of this study is how cultural dimensions shape employees’ interpretations of cybervetting in nuanced and non-deterministic ways. While prior research often treats cultural dimensions as predictors of attitudes toward privacy and organizational practices (Taras, Kirkman, & Steel, 2010), the findings suggest that these dimensions function less as fixed determinants and more as interpretive resources that individuals draw on to make sense of cybervetting. Although collectivism and uncertainty avoidance provide important context, the most significant insight concerns power distance.

Contrary to dominant assumptions, power distance does not necessarily lead to straightforward acceptance of cybervetting. While participants demonstrated clear recognition of hierarchical authority in workplace interactions, this did not translate into unconditional acceptance of employer surveillance. This challenges conventional interpretations of Geert Hofstede’s power distance dimension, which often associates high power distance with deference

to authority and compliance with organizational practices. Instead, participants consistently distinguished between respecting authority and agreeing with its actions, indicating that deference does not necessarily imply acceptance.

This distinction is critical. Existing research has increasingly questioned deterministic applications of cultural dimensions, arguing that individuals within high power-distance contexts do not passively accept authority, but actively interpret and negotiate its legitimacy (Kirkman, Lowe, & Gibson, 2006; Taras, Kirkman, & Steel, 2010). The findings of this study reinforce this critique by suggesting that recognition of authority operates alongside evaluative judgment, rather than replacing it. Participants acknowledged hierarchical structures as legitimate, yet simultaneously assessed whether specific practices, such as cybervetting, fell within acceptable boundaries of that authority.

Participants' responses indicate that power distance shapes how authority is recognized, but not how it is evaluated. Employees may conform to hierarchical norms in interactional settings—using respectful language, observing status differences, and accepting organizational structures—while still critically questioning the scope and appropriateness of employer actions. This refinement also clarifies how pragmatic privacy compliance takes shape in culturally specific ways. Deference that coexists with private reservation is not cultural contradiction; it is one of the interpretive forms through which compliance under structural constraint becomes expressible. Cultural dimensions, in this sense, do not determine whether compliance occurs. They shape the vocabulary and moral register through which compliance is enacted and through which reservation is quietly preserved.

Practical Implications

The findings of this study have important implications for organizations, employees and job seekers, policymakers, and practitioners engaged in cybervetting practices. A central insight is that employee compliance with cybervetting should not be interpreted as acceptance or endorsement. Instead, the concept of pragmatic privacy compliance highlights that individuals may outwardly comply with privacy-invasive practices due to structural constraints, while internally experiencing discomfort or resistance. As such, organizations that rely on cybervetting risk misinterpreting compliance as trust, potentially overlooking underlying concerns that may affect employee morale, organizational commitment, and perceptions of fairness.

For organizations, this study underscores the importance of transparency and contextual sensitivity in the implementation of cybervetting practices. Clearly communicating the purpose, scope, and criteria of cybervetting can reduce uncertainty and mitigate perceptions of intrusion. In addition, organizations should carefully consider the relevance of social media data to job roles, ensuring that evaluation practices are aligned with professional requirements rather than extending unnecessarily into personal domains. Establishing clear boundaries between personal and professional contexts can help maintain trust while still allowing organizations to meet their screening objectives.

The findings from this study are particularly significant for employees and job seekers. While organizations have a responsibility to develop and implement ethical cybervetting practices, individuals must also exercise caution in how they present themselves on social media. Given that online profiles can increasingly shape employment opportunities and professional perceptions, users should be mindful of the content they share and the digital footprints they create over time. This does not mean individuals should avoid authentic self-expression; rather, it

highlights the importance of understanding that personal online spaces can be subject to professional scrutiny. By managing their online presence thoughtfully, employees and job seekers can better reduce the risk of misinterpretation or unfair judgments during recruitment processes.

For policymakers and regulatory bodies, the findings highlight the need for stronger guidelines around digital privacy and data use in employment contexts. As institutional access to personal data becomes increasingly normalized, there is a growing risk that such practices will expand without adequate safeguards. One important step legislative bodies could take is to create and enforce comprehensive data protection acts that limit unnecessary access to individuals' personal information and regulate practices that encroach upon personal privacy. Policies that clearly define acceptable limits for cybervetting, protect individuals from excessive data collection, and require informed consent can help balance organizational interests with individual privacy rights.

Finally, the study suggests that practitioners should recognize the cultural and structural context within which cybervetting operates. In environments where hierarchical authority and economic pressures constrain resistance, employees may feel unable to question or refuse such practices. As a result, ethical cybervetting requires not only procedural transparency, but also an awareness of the power dynamics that shape employees' ability to respond. Addressing these dynamics is essential for ensuring that cybervetting practices are not only effective but also perceived as legitimate and fair.

Limitations and Future Research

While this study offers important insights into how employees interpret and respond to cybervetting, it also opens several directions for future research. First, the study is based on a

qualitative sample of Nigerian employees, which enables a rich, in-depth understanding of participants' experiences and meaning-making processes. However, given the size and diversity of Nigeria's workforce, these findings are not intended to be representative of the experiences of the millions of employees across the country. In addition, they cannot be assumed to reflect experiences in other national or regional contexts, where cultural, institutional, and economic conditions may differ significantly. Building on this, future research could employ quantitative or mixed-method approaches to engage larger and more diverse samples within Nigeria, thereby enhancing the generalizability of these findings and extending the applicability of the study's insights.

Second, this study focuses primarily on employees' perspectives, highlighting how cybervetting is experienced and interpreted from the standpoint of those subject to it. This creates an important opportunity for future research to examine cybervetting from the organizational perspective, particularly how employers interpret, justify, and operationalize these practices. Investigating how decision-makers conceptualize legitimacy, fairness, and risk would provide a more comprehensive understanding of cybervetting as a relational process, shaped by the interaction between organizational priorities and employee expectations.

Exploring the organizational side would also allow future studies to examine potential mismatches between how cybervetting is intended and how it is experienced. For instance, practices that organizations view as necessary for risk management may be perceived by employees as intrusive or misaligned with contextual norms of privacy. Understanding these divergences would offer valuable insight into how cybervetting practices can be designed and implemented in ways that balance organizational objectives with employee perceptions of fairness and legitimacy.

Third, the sampling strategy employed in this study opens an additional avenue for future research. In addition to purposive sampling, snowball sampling was used to recruit participants, which was effective in accessing individuals who met the study's criteria. However, because snowball sampling relies on participant networks, it may have introduced a degree of homogeneity, potentially limiting the diversity of perspectives represented in the data (Biernacki & Waldorf, 1981). While efforts were made to recruit participants across a range of industries to capture variation in experiences, future research could build on this work by employing a more strictly purposive sampling strategy. Such an approach would allow for more deliberate selection across diverse professional, demographic, and social groups, thereby broadening the range of viewpoints and further strengthening the robustness of the findings.

This study examined how employees in Nigeria perceive cybervetting, the factors shaping these perceptions, and the role of cultural dimensions or values in informing how the practice is interpreted. The findings show that cybervetting is not understood as inherently acceptable or unacceptable. Rather, participants actively evaluated its legitimacy based on contextual considerations such as platform type, job relevance, and transparency. In this sense, perceptions of cybervetting are constructed through ongoing, situational judgments about appropriateness and fairness.

At the level of experience, cybervetting was widely interpreted as extending organizational authority into personal digital spaces, thereby blurring the boundary between personal and professional life. This expansion raised concerns about privacy, the erosion of contextual boundaries, and the risk of misinterpretation when online content is evaluated outside of its original setting. Participants emphasized that meaning is context-dependent, and that removing content from its intended audience and circumstances increases the likelihood of

inaccurate judgments. As such, cybervetting was understood not simply as accessing information, but as reshaping the conditions under which that information is interpreted.

Beyond individual perceptions, responses to cybervetting were shaped by broader structural and normative conditions. Economic positioning constrained the extent to which participants could act on their privacy concerns, often resulting in compliance driven by necessity rather than genuine acceptance. Similarly, the normalization of institutional access to personal data contributed to the perception of cybervetting as part of a wider system of data extraction. Moral framings of responsibility further shaped acceptance by positioning individuals as accountable for their online presence and therefore subject to scrutiny.

With respect to culture, cultural values such as collectivism, uncertainty avoidance, and power distance influenced how participants interpreted cybervetting, though not in deterministic ways. Collectivist orientations sometimes supported acceptance, particularly when cybervetting was framed in relation to organizational reputation and group responsibility. However, power distance did not translate into uncritical acceptance of employer intrusion, despite evident deference to authority in other domains. Similarly, uncertainty avoidance was expressed in a context-dependent manner, with participants initially tolerating ambiguity but resisting when outcomes were perceived as intrusive or misaligned with expectations of fairness and privacy.

A central contribution of this study is the distinction between compliance and acceptance. Participants frequently navigated a tension between personal beliefs and economic realities, resulting in what can be understood as pragmatic privacy compliance. This finding extends Hofstede's Cultural Dimensions Theory by suggesting that cultural values alone cannot fully account for employees' responses to cybervetting. Instead, these responses emerge through the interaction of cultural orientations, structural constraints, and context-specific evaluations.

Overall, this study contributes to the literature by providing a contextually grounded account of cybervetting in an underexplored African setting. The findings highlight the need to understand cybervetting as a socially embedded practice with implications for privacy, fairness, and organizational trust. Practically, this underscores the importance of transparency, clearer boundaries around personal data, and more ethically grounded approaches to online screening. Future research can build on this work by engaging more diverse samples, incorporating employer perspectives, and further examining how cultural and structural factors shape interpretations of digital surveillance in the workplace.

Conclusion

This study examined how employees in Nigeria perceive cybervetting, the factors shaping these perceptions, and the role of cultural dimensions or values in informing how the practice is interpreted. The findings show that cybervetting is not understood as inherently acceptable or unacceptable. Rather, participants actively evaluated its legitimacy based on contextual considerations such as platform type, job relevance, and transparency. In this sense, perceptions of cybervetting are constructed through ongoing, situational judgments about appropriateness and fairness.

At the level of experience, cybervetting was widely interpreted as extending organizational authority into personal digital spaces, thereby blurring the boundary between personal and professional life. This expansion raised concerns about privacy, the erosion of contextual boundaries, and the risk of misinterpretation when online content is evaluated outside of its original setting. Participants emphasized that meaning is context-dependent, and that removing content from its intended audience and circumstances increases the likelihood of

inaccurate judgments. As such, cybervetting was understood not simply as accessing information, but as reshaping the conditions under which that information is interpreted.

Beyond individual perceptions, responses to cybervetting were shaped by broader structural and normative conditions. Economic constraints limited participants' ability to act on their privacy concerns, often resulting in compliance driven by necessity rather than genuine acceptance. Similarly, the normalization of institutional access to personal data contributed to the perception of cybervetting as part of a wider system of data extraction. Moral framings of responsibility further shaped acceptance by positioning individuals as accountable for their online presence and therefore subject to scrutiny.

With respect to culture, cultural values such as collectivism, uncertainty avoidance, and power distance influenced how participants interpreted cybervetting, though not in deterministic ways. Collectivist orientations sometimes supported acceptance, particularly when cybervetting was framed in relation to organizational reputation and group responsibility. However, power distance did not translate into uncritical acceptance of employer intrusion, despite evident deference to authority in other domains. Similarly, uncertainty avoidance was expressed in a context-dependent manner, with participants initially tolerating ambiguity but resisting when outcomes were perceived as intrusive or misaligned with expectations of fairness and privacy.

A central contribution of this study is the distinction between compliance and acceptance. Participants frequently navigated a tension between personal beliefs and economic realities, resulting in what can be understood as pragmatic privacy compliance. This finding extends Hofstede's Cultural Dimensions Theory by suggesting that cultural values alone cannot fully account for employees' responses to cybervetting. Instead, these responses emerge through the interaction of cultural orientations, structural constraints, and context-specific evaluations.

Overall, this study contributes to the literature by providing a contextually grounded account of cybervetting in an underexplored African setting. The findings highlight the need to understand cybervetting as a socially embedded practice with implications for privacy, fairness, and organizational trust. Practically, this underscores the importance of transparency, clearer boundaries around personal data, and more ethically grounded approaches to online screening. Future research can build on this work by engaging more diverse samples, incorporating employer perspectives, and further examining how cultural and structural factors shape interpretations of digital surveillance in the workplace.

References

- Abbas, S. M., & Sharma, T. (2023). Nigerian and Indian workers' study on national culture and work values: Empirical evidence with special reference to Hofstede's dimensions. *International Journal of Research in Social Sciences*, 13(4), 719–729.
- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Akbulut, Y., Esiyok, E., & Dursun, O. O. (2024). Employer and employee perceptions of cybervetting in Turkey: A mixed-methods approach. *Journal of Human Resource and Organizational Development*, 41(1), 33–52.
- Albishri, N., Chotia, V., Galgotia, A., Sahore, N., & Felicián, P. M. (2025). Cybervetting and Digital Footprints in Talent Acquisition: A Media Narrative Perspective on Information Management in Recruitment. *Journal of Global Information Management (JGIM)*, 33(1), 1-34. <https://doi.org/10.4018/JGIM.388745>
- Balcerak, A., Woźniak, J., & Zbucha, A. (2023). Predictors of fairness assessment for social media screening in employee selection. *Journal of Entrepreneurship Management and Innovation*, 19(2), 99–126. <https://doi.org/10.7341/20231923>
- Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5), 313–324. <https://doi.org/10.1080/01972240490507956>
- Berkelaar, B. L. (2014). Cybervetting, person–environment fit, and personnel selection: Employers' surveillance and sensemaking of job applicants' online information. *Journal of Business and Psychology*, 29(2), 205–219.

- Berkelaar, B. L. (2017). Theoretical frameworks for understanding cybervetting. In *The Routledge Companion to Labor and Media* (pp. 263–271). Routledge.
- Berkelaar, B. L., & Buzzanell, P. M. (2015). Online Employment Screening and Digital Career Capital: Exploring Employers' Use of Online Information for Personnel Selection: Exploring Employers' Use of Online Information for Personnel Selection. *Management Communication Quarterly*, 29(1), 84-113. <https://doi.org/10.1177/0893318914554657>
- Berkelaar, B. L., & Harrison, M. A. (2017). Cybervetting. In C. R. Scott & L. Lewis (Eds.), *The international encyclopedia of organizational communication* (pp. 1–7). Hoboken, NJ: Wiley.
- Beugelsdijk, S., Kostova, T., & Roth, K. (2017). An overview of Hofstede-inspired country-level culture research in international business since 2006. *Journal of International Business Studies*, 48, 30–47. <https://doi.org/10.1057/s41267-016-0038-8>
- Biernacki, P., & Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. *Sociological Methods & Research*, 10(2), 141–163. <https://doi.org/10.1177/004912418101000205>
- Black, J., Eschleman, K. J., & Murray, K. A. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Social Psychology*, 155(1), 62–72.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Brockner, J., Ackerman, G., Greenberg, J., Gelfand, M. J., Francesco, A. M., Chen, Z. X., Leung, K., Bierbrauer, G., Siegel, P. A., & Shapiro, D. (2001). Culture and procedural

- justice: The influence of power distance on reactions to voice. *Administrative Science Quarterly*, 46(4), 533–556. <https://doi.org/10.2307/3094872>
- Broughton, A., Foley, B., Ledermaier, S., & Cox, A. (2013). *The use of social media in the recruitment process*. Institute for Employment Studies.
- Brown, V. R., & Vaughn, E. D. (2011). The writing on the (Facebook) wall: The use of social networking sites in hiring decisions. *Journal of Business and Psychology*, 26(2), 219–225. <https://doi.org/10.1007/s10869-011-9221-x>
- BusinessDay. (2024, February 8). Nigeria: Lagos leads in internet users despite economic challenges. *BusinessDay*. <https://businessday.ng/news/article/nigeria-lagos-leads-in-internet-users-despite-economic-challenges/>
- Central Bank of Nigeria. (2014). *Regulatory framework for the Bank Verification Number (BVN)*.
- Cook, R., Jones-Chick, R., Roulin, N., & O'Rourke, K. (2020). Job seekers' attitudes toward cybervetting: Scale development, validation, and platform comparison. *International Journal of Selection and Assessment*, 28(4), 383–398. <https://doi.org/10.1111/ijsa.12300>
- Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). SAGE Publications.
- Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.
- Drake, J. R. & Furner, C. P. (2020). Screening Job Candidates With Social Media: A Manipulation of Disclosure Requests. *Journal of Organizational and End User Computing (JOEUC)*, 32(4), 63-84. <https://doi.org/10.4018/JOEUC.2020100104>

- Engström, E., Forsman, M., & Ågerfalk, P. J. (2023). Cross-national differences in privacy concerns: The role of national culture and regulatory environment. *Journal of Information Security and Applications*, 73, 103439. <https://doi.org/10.1016/j.jisa.2023.103439>
- Frampton, B., & Child, J. T. (2013). Friend or not to friend: Coworker Facebook friend requests as an application of communication privacy management theory. *Computers in Human Behavior*, 29(6), 2257–2264. <https://doi.org/10.1016/j.chb.2013.05.006>
- Gerhart, B., & Fang, M. (2005). National culture and human resource management: assumptions and evidence. *The International Journal of Human Resource Management*, 16(6), 971–986. <https://doi.org/10.1080/09585190500120772>
- Gershon, I. (2017). *Down and out in the new economy: How people find (or don't find) work today*. University of Chicago Press.
- Gruzd, A., Jacobson, J., & Dubois, E. (2020). Cybervetting and the public life of social media data. *Social Media + Society*, 6(2). <https://doi.org/10.1177/2056305120915618>
- Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field Methods*, 18(1), 59–82. <https://doi.org/10.1177/1525822X05279903>
- Hartwell, C., & Campion, M. (2019). Getting social in selection: How social networking website content is perceived and used in hiring. *International Journal of Selection and Assessment*, 28(1), 1–16. <https://doi.org/10.1111/ijsa.12273>
- Hedenus, A., Backman, C., & Håkansson, P. (2021). Whom do you know? Recruiters' motives for assessing jobseekers' online networks. *The International Journal of Human Resource Management*, 32(8), 1754–1777. <https://doi.org/10.1080/09585192.2019.1579245>

- Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Jacobson, J., & Gruzd, A. (2020). Cybervetting job applicants on social media: The new normal? *Ethics and Information Technology*, 22(2), 175–195. <https://doi.org/10.1007/s10676-020-09526-2>
- Jacobson, J., & Gruzd, A. (2024). Cybervetting job applicants on social media: The new normal? *Preprint*. <https://doi.org/10.32920/25475317.v1>
- Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, 72(12), 2954-2965. <https://doi.org/10.1111/jan.13031>
- Kirkman, B. L., Lowe, K. B., & Gibson, C. B. (2006). A quarter century of culture's consequences: A review of empirical research incorporating Hofstede's cultural values framework. *Journal of International Business Studies*, 37(3), 285–320. <https://doi.org/10.1057/palgrave.jibs.8400202>
- Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage Publications.
- McDonald P, Thompson P & O'Connor P (2016) Profiling employees online: shifting public-private boundaries in organizational life. *Human Resource Management Journal*, 26 (4), pp. 541-556. <https://doi.org/10.1111/1748-8583.12121>
- McDonald, N., DeVries, I., & Rader, E. (2021). More than just privacy: Unpacking the personal and societal benefits of social media vetting in hiring. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 1–22. <https://doi.org/10.1145/3449153>

- Morrison, E. W. (2014). Employee voice and silence. *Annual Review of Organizational Psychology and Organizational Behavior*, 1, 173–197. <https://doi.org/10.1146/annurev-orgpsych-031413-091328>
- Mujtaba, B. G. (2023). Digital literacy on privacy rights policies in the American workplace. In P. Vardarlier (Ed.), *Multidimensional and strategic outlook in digital business transformation* (pp. [insert page range]). Springer. https://doi.org/10.1007/978-3-031-23432-3_10
- Nigerian Communications Commission. (2020). *Revised SIM registration guidelines*.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Noy, C. (2008). Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of Social Research Methodology*, 11(4), 327–344. <https://doi.org/10.1080/13645570701401305>
- Olatunji, F. O. (2015). Culture and surveillance in Nigerian workplaces. *Journal of African Cultural Studies*, 27(3), 313–330.
- Omoju, O. E., et al. (2023). Empirical review of youth-employment policies in Nigeria. *arXiv*. <https://arxiv.org/abs/2310.07789>
- Otiwa, J., Edet, S., & Adomokhai, S. S. (2021). Hofstede’s cultural dimensions and implications for entrepreneurial development in Nigeria. *Journal of Management & Entrepreneurial Studies*, 2(1–4), 119–132.
- Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.

- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.
- Phillippi, J., & Lauderdale, J. (2018). A guide to field notes for qualitative research: Context and conversation. *Qualitative health research*, 28(3), 381-388.
<https://doi.org/10.1177/1049732317697102>
- Price, R. A. (2019). *Youth employment needs in Nigeria* (K4D Helpdesk Report 691). Institute of Development Studies.
- Robards, B., & Graf, D. (2022). “How a Facebook update can cost you your job”: News coverage of employment terminations following social media disclosures, from racist cops to queer teachers. *Social Media + Society*, 8(1).
<https://doi.org/10.1177/20563051221077022>
- Roulin, N., & Liu, Z. (2023). Job seekers’ attitudes toward cybervetting in China: Platform comparisons and relationships with social media posting habits and individual differences. *International Journal of Selection and Assessment*, 31(2), 347–354.
<https://doi.org/10.1111/ijsa.12424>
- Rózsa, Z., & Kmecová, I. (2020). Cybervetting prospective employees of SMEs. *Journal of International Studies*, 13(1), 295–309. <https://doi.org/10.14254/2071-8330.2020/13-1/19>
- Sallach, T., Mönke, F. W., & Schäpers, P. (2024). Cybervetting of organizational citizenship behavior expectations: Profile summary as a key in LinkedIn-based assessments. *Computers in Human Behavior*, 154, 108113. <https://doi.org/10.1016/j.chb.2023.108113>
- Schäpers, P., Mönke, F. W., Frieler, C.-M., Roulin, N., & Basch, J. (2025). Attitudes toward cybervetting in Germany: Impact on organizational attractiveness depends on social

- media platform. *International Journal of Selection and Assessment*, 33(1), e70003.
<https://doi.org/10.1111/ijsa.70003>
- Scott, J. C. (1985). *Weapons of the weak: Everyday forms of peasant resistance*. Yale University Press.
- Smith, P. When elephants fight, the grass gets trampled: the GLOBE and Hofstede projects. *J Int Bus Stud* 37, 915–921 (2006). <https://doi.org/10.1057/palgrave.jibs.8400235>
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.
- Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly*, 30(3), 679–704. <https://doi.org/10.2307/25148745>
- Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology*, 30(1), 73–88.
- Straub, D., Keil, M., & Brenner, W. (1997). Testing the technology acceptance model across cultures: A three country study. *Information & Management*, 33(1), 1–11.
[https://doi.org/10.1016/S0378-7206\(97\)00026-8](https://doi.org/10.1016/S0378-7206(97)00026-8)
- Taras, V., Kirkman, B. L., & Steel, P. (2010). Examining the impact of culture's consequences: A three-decade, multilevel, meta-analytic review of Hofstede's cultural value dimensions. *Journal of Applied Psychology*, 95(3), 405–439. <https://doi.org/10.1037/a0018938>
- Taras, V., Kirkman, B. L., & Steel, P. (2010). Examining the impact of culture's consequences: A three-decade, multilevel, meta-analytic review of Hofstede's cultural value dimensions. *Journal of Applied Psychology*, 95(3), 405–439. <https://doi.org/10.1037/a0018938>

- Tracy, S. J. (2019). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact* (2nd ed.). Wiley-Blackwell.
- van den Bos, K., Brockner, J., Stein, J. H., Steiner, D. D., & Kulik, C. T. (2013). Power distance and procedural justice: How general and specific cultural values shape fairness perceptions. *Journal of Cross-Cultural Psychology*, 44(8), 1294–1311.
<https://doi.org/10.1177/0022022113505356>
- van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197–208.
<https://doi.org/10.24908/ss.v12i2.4776>
- Vosen, A. J. (2021). Social media screening of job applicants: A review of fairness, legality, and ethics. *Employee Responsibilities and Rights Journal*, 33(4), 227–247.
<https://doi.org/10.1007/s10672-020-09371-2>
- Wilcox, A., Damarin, A., & McDonald, S. (2022). Is cybervetting valuable? *Industrial and Organizational Psychology*, 15(3), 315–333. <https://doi.org/10.1017/iop.2022.28>
- Wilcox, D. A., Rothwell, J. W., & Tews, M. J. (2022). Cybervetting as workplace surveillance: Ethical implications for organizations and employees. *Industrial and Organizational Psychology*, 15(2), 283–298. <https://doi.org/10.1017/iop.2021.45>
- Yao, M.Z., Rice, R.E. and Wallis, K. (2007), Predicting user concerns about online privacy. *J. Am. Soc. Inf. Sci.*, 58: 710-722. <https://doi.org/10.1002/asi.20530>
- Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.

Appendix A - Interview Protocol

Opening, Consent, and Rapport

Hello, and thank you for taking the time to talk with me today.

I am interested in how people working in Nigeria experience employers looking at their online presence, such as social media, during hiring or at work. There are no right or wrong answers here. I am interested in your experiences and perspectives.

Our conversation should last about 30 to 50 minutes. With your permission, I will record the interview so that I can focus on listening and later transcribe what you say. Your name and any identifying details will be removed from anything I write. You can skip any question or stop the interview at any time.

Before we get started, do you have any questions for me about the study or how I will use your responses?

Warm up and Background

1. To start us off, can you tell me a little about your current job or the kind of work you do?
2. How long have you been working in this field or type of job?
3. In general, how do you use social media or online platforms in your everyday life?
 - For example, for staying in touch with friends and family, professional networking, entertainment, news, and so on.

Experiences with Employers Checking Online Presence

4. Thinking about your work or job search, can you tell me about any time when an employer or recruiter checked your social media or online presence?

Probes

- What exactly happened?
- How did you first become aware that they were checking?
- How did you feel at the time?
- Has your feeling about it changed since then?
- What did you do in response, if anything?
 - For example, did you change your profiles, talk to anyone about it, or decide to ignore it?

4b. If nothing like that has happened to you personally, have you heard stories of this happening to colleagues or friends?

Probes

- Can you tell me about one example that stands out to you?
- What did you think when you heard about it?

Fairness and Acceptability

5. When you think about employers reviewing social media for hiring or promotion decisions, how does that sit with you?

Probes

- What, if anything, feels fair or acceptable about it?
 - What, if anything, feels unfair or uncomfortable?
 - Do your feelings change depending on the type of platform, for example LinkedIn versus Instagram or Facebook? In what ways?
6. In your view, should employers tell people if they are going to review their online presence?

Probes

- Why do you feel that way?
- If you believe they should tell people, what would good communication about this look like?
 - For example, what information would you expect about which platforms they will check, what they are looking for, and how they will use the information?
- How do you think you would respond if an employer clearly explained their cybervetting process to you?

Privacy

7. When employers review applicants or employees online, how do you think about privacy in that situation?

Probes

- In what ways, if any, do you see this as a violation of personal privacy?
- Are there situations where it does not feel like a privacy violation to you? What makes those situations different?
- Where would you personally draw the line between what is okay to check and what is too personal.

Economic Conditions and Tradeoffs

8. Thinking about the job market in Nigeria and your own situation, how do economic conditions affect the way you think about employers checking social media?

Probes

- If you really needed a job or were worried about losing one, how might that influence what you are willing to accept or tolerate?
- Have you ever felt you had to accept something you were not fully comfortable with because you needed the job? Can you describe what happened?
- How do you weigh privacy or fairness concerns against economic needs?

Managing Online Presence and Digital Literacy

9. How do you currently manage your online profiles in relation to your work or career?

Probes

- What kinds of things do you do, or avoid doing, because you are thinking about employers or colleagues who might see your posts?
- How confident do you feel about your ability to present yourself online in a way that supports your job prospects?
- Have you ever changed your online behavior because of something you heard or experienced about employers checking social media? What changed?

Cultural and Workplace Context

Representation and Responsibility

10. In your view, when you post online, to what extent are you representing only yourself, and to what extent are you also representing your family, community, or workplace?

Probes

- Can you give an example of a time when you felt your online behavior might reflect on your workplace or community?
- How does that sense of responsibility shape your opinion about employers reviewing social media?
- Do people around you, such as friends, family, or colleagues, talk about how their online actions can affect the reputation of their workplace?

Power and Questioning Management

11. In your workplace, how do people usually respond when management makes decisions about things like monitoring or checking employees' behavior, including online behavior?

Probes

- Can employees ask questions or push back if they disagree, or is it more common to accept decisions without saying much?
- Have you seen or experienced a situation where someone challenged a decision related to social media or online behavior? What happened?
- How comfortable would you personally feel raising concerns if you thought an employer's social media monitoring was going too far?

Rules, Policies, and Uncertainty

12. When it comes to employers checking social media, what kind of approach makes you feel more comfortable?

Probes

- Do you prefer clear rules and written policies, or are you comfortable with managers using their own judgment without formal rules? Why?
- Have you ever worked somewhere that had clear policies about social media use or monitoring? How did that affect how you behaved online?
- How would your feelings change if the rules were very strict compared with rules that were more general or flexible?

Closing and Participant Reflection

13. Is there anything we have not talked about that you think is important for understanding how people in Nigeria experience employers checking social media or other online information?

Probes

- If you could give advice to employers in Nigeria about how to handle cybervetting in a fair and respectful way, what would you tell them?
- What advice, if any, would you give to workers or job seekers about managing their online presence, given what we have discussed?

Closing Script

Thank you again for sharing your experiences and perspectives. They are very valuable for this study.

Before we end, is there anything you would like to ask me or anything you would like to add?

Appendix B - Consent Form

PROJECT TITLE:

Beyond the Resume: Perceptions of Cybervetting Among Employees in Nigeria

CT APPROVAL DATE:	PROJE	2/9/2	PROJE	02/08/2	LENG	1
	026		CT EXPIRATION DATE:	029	TH OF STUDY:	2 weeks

PRINCIPAL INVESTIGATOR:	Dr. Sean Eddington
------------------------------------	--------------------

CO- INVESTIGATOR(S):	Stanley Uzoma
---------------------------------	---------------

CONTACT DETAILS FOR PROBLEMS/QUESTIONS:	seanneddington@ksu.edu scuzoma@ksu.edu
--	--

IRB CHAIR CONTACT INFORMATION:	Lisa Rubin, Chair, Committee on Research Involving Human Subjects, 203 Fairchild Hall, Kansas State University, Manhattan, KS 66506, (785) 532-3224) Brad Woods, Associate Vice President for Research Compliance, 203 Fairchild Hall, Kansas State University, Manhattan, KS 66506, (785) 532-322
---	--

PROJECT SPONSOR:	N/A
-----------------------------	-----

PURPOSE OF THE RESEARCH:

This study aims to understand how cybervetting-- the practice of screening the social media profiles of job applicants and employees for hiring and promotion purposes-- is perceived by employees in Nigeria, and also explore what factors and cultural elements shape their perceptions.

PROCEDURES OR METHODS TO BE USED:

Through in-depth interviews with Nigerian employees, this study seeks to examine how cybervetting is perceived and how cultural and contextual factors shape these perceptions. During the interviews, participants will be invited to share their experiences with cybervetting and their views on related issues such as privacy and fairness. Additional questions will explore factors that may influence these perceptions. With participants' consent, interviews will be audio-recorded, transcribed, and analyzed thematically. Participation in the study is entirely voluntary, and all identifying information will be kept confidential.

The findings from this study may inform employers and human resources practitioners in Nigeria and similar contexts in the development of ethical cybervetting policies. Additionally, the study may provide educational value to Nigerian employees by enhancing their understanding of privacy and data protection rights in relation to cybervetting practices.

RISKS OR DISCOMFORTS ANTICIPATED:

This study involves minimal risk, and there should be no physical discomfort. The interview questions are designed to explore perception of social media screening by employees and the factors that contribute to perception. However, if you feel uneasy at any point, please know that you can skip any question you don't wish to answer. Participation is entirely voluntary, and you are free to withdraw from the study at any time without any consequences. We have designed the survey to be respectful of your time and experiences. If you do feel any discomfort, contact information for support services will be provided to assist you. Your well-being is important, and we want you to feel comfortable throughout the process.

BENEFITS ANTICIPATED:

While there may be no direct or immediate benefits to you as a participant, your involvement in this study contributes to expanding scholarship on cybervetting by addressing a significant gap focused on employees' perceptions in a sub-Saharan context. The findings may help guide employers and human resources practitioners in Nigeria and similar settings in developing ethical cybervetting policies. Additionally, your participation may provide

educational value by enhancing Nigerian employees understanding of privacy and data protection rights in relation to cybervetting practices.

EXTENT OF CONFIDENTIALITY:

Your privacy is a top priority in this study. All responses will be kept confidential, and no personally identifiable information will be collected. The data you provide will be anonymized, meaning your answers cannot be traced back to you. Only I and my supervisor will have access to the data, and it will be securely stored on password-protected servers. Your participation is entirely anonymous, and your information will not be shared with anyone outside of the research team. Your information, even if identifiers are removed, will not be used or distributed for future research studies.

[Select a statement from the drop down menu]

IS COMPENSATION OR MEDICAL TREATMENT AVAILABLE IF INJURY OCCURS? ☐ Yes ☐ No

Terms of participation: I understand this project is research, and that my participation is voluntary. I also understand that if I decide to participate in this study, I may withdraw my consent at any time, and stop participating at any time without explanation, penalty, or loss of benefits, or academic standing to which I may otherwise be entitled.

I verify that my signature below indicates that I have read and understand this consent form, and willingly agree to participate in this study under the terms described, and that my signature acknowledges that I have received a signed and dated copy of this consent form.

(Remember that it is a requirement for the P.I. to maintain a signed and dated copy of the same consent form signed and kept by the participant).

**PARTICIPANT
NAME:**

**PARTICIPANT
SIGNATURE:**

DATE:

--

**WITNESS TO
SIGNATURE: (PROJECT
STAFF)**

DATE:

Appendix C - Appendix: IRB Approval Letter



Office of Research Integrity,
Compliance and Security

TO: Sean Eddington
AQ Miller School of Media and Communication
Manhattan, KS 66506
Proposal Number IRB-13523

FROM: Lisa Rubin, Chair
Committee on Research Involving Human Subjects

DATE: 02/09/2026

RE: Approval of Proposal Entitled, "Beyond the Résumé: Perceptions of Cybervetting Among Employees in Nigeria."

The Committee on Research Involving Human Subjects has reviewed your proposal and has granted full approval. This proposal is **approved for three years from the date of this correspondence.**

APPROVAL DATE: 02/09/2026

EXPIRATION DATE: 02/08/2029

In giving its approval, the Committee has determined that:

No more than minimal risk to subjects

This approval applies only to the proposal currently on file as written. Any change or modification affecting human subjects must be approved by the IRB prior to implementation. All approved proposals are subject to continuing review, which may include the examination of records connected with the project. Announced post-approval monitoring may be performed during the course of this approval period by URCO staff. Injuries, unanticipated problems or adverse events involving risk to subjects or to others must be reported immediately to the Chair of the IRB and / or the URCO.

Electronically signed by Lisa Rubin on 02/09/2026 3:07 PM ET