2022

Safeguarding Employee Privacy in U.S.-Based Small and Midsized Businesses

Kim de Peiza
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Kim de Peiza

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Allen Endres, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Alexandre Lazo, Committee Member, Doctor of Business Administration Faculty

Dr. Yvonne Doll, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Safeguarding Employee Privacy in U.S.-Based Small and Midsized Businesses

by

Kim de Peiza

MS, Walden University, 2007

BS, University of Phoenix, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

September 2022

Abstract

Employee privacy is a contentious concern between employees and employers in the United States. Terminating oversurveilled employees may result in sustained claim costs for a company. Grounded in complexity theory and complexity leadership theory, the purpose of this qualitative multiple case study was to explore strategies small business leaders/agents use to safeguard employee privacy. The participants included three privacy practitioners: one consultant, and two small business leaders/agents of small businesses in the Mid-Atlantic U.S. region who had successfully safeguarded employee privacy. A thematic analysis using primary and secondary sources identified three principal themes: (a) environmental privacy, (b) autonomy privacy, and (c) personal information privacy. A key recommendation is for business leaders to design a human-centric employee privacy program with defensive and offensive strategies that balance autonomy with accountability. This study has implications for positive social change in that it may inform efficacious strategy to promote employee privacy that catalyze employee innovation and improve business performance, enabling organizations to sustain their contributions to benefit the citizens of their local community.

Safeguarding Employee Privacy in U.S.-Based Small and Midsized Businesses

by

Kim de Peiza

MS, Walden University, 2007

BS, University of Phoenix, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

September 2022

Dedication

Thanking GOD for all things and placing GOD above everything.

I dedicate this study to my grandpa, Mr. Martin Matthews, a consummate educator from the lovely isle of Dominica; my father, Steve Leslie John; and my maternal grandmother, Vida Herbert Matthews.

Acknowledgments

"The defense of privacy will be the savior of the future, essentially." Svea Eckert

To those who saw me start and finish this journey and provided august support. To my mom, who is perhaps the proudest person who accompanied me throughout this journey. To my husband, who held the fort on many weekends. My success team, Maxime, Dale, Carla, Kiesha, Karen, Christine, Cheryl, Michelle and other cheerleaders.

To my Walden University committee chair, Dr. Allen Endres; my second committee member, Dr. Alexander Lazo; my University Research Reviewer (URR), Dr. Yvonne Doll; and my academic advisor, Dr. Rick Hay, thanks for being active listeners, leading with courage, and standing in the gap, so that I was able to complete this journey with grace.

To the three participants who volunteered for my research and were critical to my success. Thanks for trusting me and sharing your experiences and practices on safeguarding employee privacy so that I might complete this study and share findings with the academic and business communities. I wish all of you the very best in your efforts to grow your businesses.

Table of Contents

List of Tables

Section 1: Foundation of the Study

A volatile social context, unchecked advancements in datafication practices, incessant breaches that expose the personal data of data subjects, a pandemic, a rise in mental health awareness, the rise of surveillance capitalism, and privacy invasions have all culminated in rapid changes in citizen requirements and expectations, business modeling, market dynamics, and new regulatory and compliance issues. As aptly noted in a report by the United Nations Global Pulse on Big Data for Development (2012), “Because privacy is a pillar of democracy, we must remain alert to the possibility that it might be compromised by the rise of new technologies and put in place all necessary safeguards” (p. 24).

The business agents for the 21st century may therefore balance their need for protecting corporate assets and determining productivity with the risks associated with ubiquitous computing, pervasive surveillance, incessant breaches, and the wellness implications of a perceived undermining of employee privacy. By using a blended framework of complexity sciences/theory (CT) and complexity leadership theory (CLT) to explore the safeguarding of the employee privacy phenomena within small to midsized firms, it may be possible to discover themes that facilitate organizational longevity and community prosperity.

Background of the Problem

Attacks on privacy through intrusions and incessant breaches, along with social unrest, a rise in the need for mental wellness, and the COVID-19 pandemic, have formed the perfect storm for conversations around regulations and institutional behaviors pertaining to privacy, risk, and security. According to Bodie (2022), the type, sourcing and extraction of data types and the speed and volume of analytics have changed astoundingly over time. New ideas of organizational controllability, business modeling, employee privacy limitations, work design, trust, compassion, and employee-employer relations, are being revisited due to increasing uncertainty and concern for needed resolutions around the use of surveillance technologies and digital wellness (Bodie, 2022; Katsabian, 2020; Tewes, 2017; Turner, 2020; Wheatley, 2017). This revisitation, during the confluence of social and individual awareness regarding the notion of privacy, against the perceived tensions of corporate requests that may intrude on the private affairs boundaries of employees who are currently in a new work design, provides an opportunity for business leaders/agents to develop and implement more relevant and viable designs.

The clandestine use of technological capabilities such as ubiquitous computing, fitness and wellness wearables, electronic monitoring and surveillance systems, and third-party trading of personal data by business practitioners should be explored, and the negative implications of such practices for various stakeholders should be addressed. The tensions between the extraction of personal data from unwitting data subjects have moved from the consumer realm into the employer–employee dynamic (Turner, 2020). In the United States, small and midsized businesses (SMBs) employed 60.6 million people, or 47.1% of the private workforce, in 2017 (Small Business Administration, 2020). Lack of privacy is a major source of worker dissatisfaction, especially in the environmental dimension (Weber et al., 2021). By imposing this issue into the volatility, ambiguity, chaos, and uncertainties of this period, researchers can describe, explore, and unearth new issues or provide sound options for crafting alternative ways forward, through the development of new paradigms for sensemaking and decision making, and leadership capabilities.

New business models and offerings may emerge that could result in business ethics that are morally palatable and support organizational sustainability. Business leaders/agents and various data subjects/owners are re-engineering their expectations in transactions. Cybersecurity alone is not sufficient to alleviate this undermining of trust. As such, the National Institute of Standards and Technology (NIST) has integrated privacy considerations into the basic control suites that many organizations now rely on. Further, NIST intentionally added the word "privacy" to the title of the *NIST Cybersecurity and Privacy Annual Report* for FY2020. This addition reflected changing technological capabilities and societal expectations (NIST, 2020). New thinking is being applied to the current space, and new rules of engagement are being formulated and debated (Backlander, 2020; Katsabian, 2020; Wheatley, 2011). We are approaching a more assertive era for the preservation of privacy from various stakeholders.

Given this current context, the social researcher, as a change leader/agent, could have new assumptions, philosophies and guiding principles, tools, techniques, and tactics and use them to craft solutions for the 21st century. Business leaders/agents who recognize their role and responsibility in crafting organizational activities that are centered on the human factor, designed for trust and digital wellness during exchanges, could exemplify new rules for employee–employer relations pertaining to safeguarding employee privacy in the United States. The background to the problem has been provided, and the focus will now shift to the problem statement.

Problem Statement

Workplace privacy is a contentious concern between employees and employers (Bhave et al., 2020, p. 6). For example, in the United States, the termination of an oversurveilled employee can cost a company more than $500,000 for the employee’s lost wages (Tomczak et al., 2018, p. 252). The general business problem is that the performance of multiple SMBs is adversely affected by employees’ workplace privacy issues. The specific business problem is that some SMB leaders lack effective strategies to safeguard employee privacy.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the effective strategies that SMB leaders use to safeguard employee privacy. The targeted population for this study consisted of two participant groups—consultants and corporate governance team members (C-suite members). I interviewed three qualified participants from April 2022 to March 2022. The interviewees consisted of one consultant of small to large businesses in the tech sector and two C-suite leaders/agents from two separate SMBs located in the Mid-Atlantic region of the United States who had successfully developed and implemented strategies for safeguarding employee privacy within their organizations. The findings of the study could support social change by enabling SMB leaders to develop strategies for assuring the privacy of employees, along the dimensions of personal information, autonomy, and environment. Assuring employees’ privacy can increase employee morale, trust, and commitment during organizational exchanges, improving business performance and management relations (Hornberger, 2021). Improved business performance enables organizations to sustain their contributions to benefit the citizens of their local communities.

Nature of the Study

I chose the qualitative method for my study. According to Matt et al. (2017), using the qualitative method enables the development of descriptions that are important to characterize dynamic processes. Researchers use the qualitative method to explore contemporary, real-life situations, identify the significance of events, answer questions, and capture descriptions of human experiences from plural perspectives in the naturalistic setting for the phenomenon being studied (Cook, 2017; Crane et al., 2018). Alternatively, the quantitative method is appropriate when researchers use research measurement to evaluate hypotheses, analyze relationships among variables, and make predictions and generalizations (Edwards-Brown, 2020). Therefore, the quantitative method was not suitable for my study because the purpose of my study was to describe the privacy-safeguarding strategies of SMBs, and not to examine variables' relationships about the privacy phenomenon in SMBs. According to Saunders et al. (2019), the mixed-method approach uses both quantitative and qualitative research methods to address complicated research questions and develop a deeper theoretical understanding. As such, the mixed method was not appropriate for my study because I did not need the quantitative method to identify and explore the effective strategies that SMB leaders used to safeguard employee privacy.

I chose a qualitative multiple case study design for my study. I also considered the appropriateness of the ethnographic and phenomenological designs. Through a qualitative multiple case study design, a researcher can explore *what, how,* and *why* and obtain details and perspectives concerning a specific situation replicated across more than a single case (Yin, 2018). Using the multiple case study research design, a researcher can also capture rich perspectives on the various human capital management strategies employed at various levels of the organization and can strengthen understanding of the patterns of findings through reproduction across many cases (Yin, 2018). A single case study, as posited by Gustafsson (2017), would not have provided me with the depth and breadth of information on this employee privacy phenomenon. Use of the miniethnographic design requires a researcher to be immersed in the culture and use participant-observation as a data collection instrument (Fusch et al., 2017). The miniethnographic design was not a fit for my study, because I did not immerse myself in the organizational context, as a participant observer, or in receipt of the safeguarding strategies for employees in the selected SMBs. Through the phenomenological design, researchers explore the meaning of lived experiences of an individual or group of people related to a unique phenomenon (Cook, 2017). The phenomenological design was not appropriate because I did not need to explore the personal meanings of participants' lived experiences during this study.

Research Question

The primary research question for this study was the following: What effective strategies do SMB leaders use to safeguard employee privacy?

Interview Questions

I conducted three interviews in total. I conducted two semistructured interviews with open-ended questions with the two C-suite participants. I also conducted one semistructured interview with open-ended questions with the one consultant participant.

The following were the interview questions for the two groups of participants:

Privacy Practitioner—Interview Questions for C-Suite Participants

1. What leadership strategies do you use to effectively safeguard employee privacy?
2. What strategies do you use to handle employee privacy in a remote work design?
3. What leadership strategies do you use to effectively safeguard the privacy of employees when using corporate surveillance tools?
4. What strategies do you use to gain buy-in and resources from your organization to ensure employee privacy is safeguarded?
5. How is the effectiveness of your employee privacy strategies assessed?
6. What supporting organizational processes do you use to determine if your policies and strategies are being effective?
7. What were the key barriers to implementing the employee privacy strategy?
8. How did you address the key barriers to implementing the employee privacy strategy?
9. What other information would you like to share about the strategies you developed and implemented to effectively safeguard employee privacy?

The following were the interview questions I asked specifically to the consultant participants:

Privacy Practitioners—Interview Questions for Consultants

1. What size of organizations have you supported for employee privacy initiatives?
2. From what sectors are most of your clients?
3. What is the focus of your consulting on employee privacy?
4. What information can you tell me about your consulting experiences with employee privacy?
5. As you are able, please identify two small or midsized company websites with robust employee privacy policies that you can recommend to me?
6. As you are able, please tell me which privacy practitioner can you refer me to from either a small or midsized company that you may have supported, so that their exemplary strategies and perspectives may be included in my study?

Conceptual Framework

The composite conceptual framework that I chose for my study was complexity theory/sciences (CT) and complexity leadership theory (CLT). Complexity science is an amalgamation of several new perspectives that have emerged in the physical and natural sciences (Mathews et al., 1999). CT may be used as a lens through which organizations are viewed as complex systems that cannot be observed using traditional linear methodologies (Turner & Baker, 2019). During the 1990s, researchers extended and adopted CT into the social sciences, and then they applied it to organizational leadership and processes (Uhl-Bien, 2021). Researchers use CT as a bridge between the natural and social sciences and apply it to view organizations as complex adaptive systems. Complexity has not been defined, except in a metaphorical manner against natural occurrences in various hard scientific fields of biology, chemistry, and physics, to name a few (Rosenhead et al., 2019; Zimmerman et al., 2008).

CT has key tenets. The key constructs underlying CT are (a) an amalgamation of various theories, (b) the butterfly effect, (c) fractals, (d) nonlinearity, and (e) viewing organizations as complex adaptive systems (Zimmerman et al., 2008). Guiding principles of CT are (a) clockware versus swarmware, (b) wicked questions, (c) nonlinearity, (d) interconnectedness, (e) diverse, (f) learning—intuitive and known knowledge, and (g) coevolution (Zimmerman et al., 2008). These tenets and principles support organizational responses in these volatile, chaotic, and uncertain times.

CLT is a leadership model that is complementary with CT and accepts complexity. CLT provides powerful, flexible mental models for developing strategies to guide organizational inquiry and adaptive responses to changing business conditions (Hazy & Prottas, 2018; Zimmerman et al., 2008). The complexity leadership (CL) framework proposed by Marion and Uhl-Bien in 2001 includes adaptive, generative, administrative, and enabling leadership theories (Hazy & Prottas, 2018). According to Uhl-Bien (2021), CLT addresses all Rost's 1993 typology for leadership—the nature of leadership as relational; the peripheral elements of leadership for individual and organizational adaptability; and "content"-complexity leadership mindsets, behaviors, and styles. CL appreciates the nature and behaviors of the agents of change in any capacity—leaders or followers—for shared leadership (Zhu et al., 2018), and mindfully uses levers to craft relevant adaptive responses. CLT encompasses leadership as a multilayered dynamic system of collaboration and coordination; as acts of spontaneous, bottom-up, emergent responses and continuous acts of relational and connected accomplishments.

Operational Definitions

Clockware: Clockware are standardized controlled, and measured processes (Zimmerman et al., 2008).

Complex adaptive system: A complex adaptive system is a complex, nonlinear, interactive system that adapts to a changing environment (Zimmerman et al., 2008).

Digital wellness (also known as *digital wellbeing* or *digital health*): Digital wellness is the pursuit of an intentional and healthy relationship with technology in the workplace and in personal life (https://www.citrix.com/glossary/what-is-digital-wellness.html).

Employee privacy: Employee privacy has been defined by E. F. Stone and Stone (1990) as a state or condition in which individuals have the capacity to (a) control the release and possible subsequent dissemination of information about themselves, (b) regulate both the amount and nature of social interaction, (c) exclude or isolate themselves from unwanted (auditory, visual, etc.) stimuli in an environment, and, as a consequence, (d) behave autonomously (i.e., free from the control of others), which arises out of the employer–employee exchange and has three dimensions—personal information, autonomy, and environment (Bhave et al., 2020).

Generative relationships: Generative relationships are human relationships that produce new sources of value that cannot be foreseen in advance (Zimmerman et al., 2008).

Personal data: Personal data include a person's name, address, phone, date of birth, and email (*personally identifiable information* [PII]), as well as economic, social, cultural, genetic, and mental characteristics (i.e., *sensitive information* [SI]). Photos, bank details, posts on social networking websites, political opinions, health information (HI), computer IP addresses, and more also are considered personal data (Kirk, 2018).

Privacy as a Right: Privacy as a Right, determined in 1965 by the Supreme Court of the United States, described privacy as a fundamental right (Yin et al., 2018).

Swarmware: Swarmware are the outcomes of processes including experimentation, trial, and error, and the balanced risk taking and autonomy of agents (Zimmerman et al., 2008).

Surveillance capitalism: According to Zuboff (2019), surveillance capitalism may be defined as follows:

> 1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; 2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modifications; 3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; 4. The foundational framework of a surveillance economy; 5. As significant a threat to human nature in the twenty-first century as

> industrial capitalism was to the natural world in the nineteenth and twentieth; 6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; 7. A movement that aims to impose a new collective order based on total certainty; 8. An expropriation of critical human rights that is best understood as a coup from above; an overthrow of the people's sovereignty. (p. vi)

Assumptions, Limitations, and Delimitations

Assumptions

Jansson (2013) noted that research assumptions are ideas that a researcher has accepted as true and that convey risks. In this doctoral study, I made five assumptions:

1. The review of public-facing documents, the literature review, and the semistructured interviews would provide sufficient data to answer the overarching research question and would be sufficient for triangulation.
2. I would be able to reduce or eliminate the effect of personal bias. To increase this probability, I used triangulation for reliability and validity and suspended my beliefs.
3. Participants would provide honest and detailed responses to interview questions.
4. I would be able to conduct effective interviews and solicit authentic responses from the participants. To increase this probability, I discussed how confidentiality would be preserved and that the participant volunteers could withdraw from the study at any time, with no ramifications.

5. The sample was representative of the population selected. To increase this probability, I verified through my professional network that offices of participating small business leaders/agents were in the Mid-Atlantic region in the United States. Privacy consultants and business leaders/agents are most knowledgeable to describe privacy safeguarding strategies for employees.

If any of these assumptions had been determined to be violated, then I would have had to review the methodology, the study design, and/or the data analysis technique.

Limitations

Limitations refer to potential weaknesses of a study that are not within the researcher's control. Limitations may be outflows of the methodology and study design selected (Simon, 2011). An inherent limitation of the selected qualitative methodology was that it might not be replicable (Simon & Goes, 2013). Another limitation was that the result of a case study design is not generalizable (Simon & Goes, 2013). The case study design requires interviews, for which face-to-face format is preferred (Saunders et al., 2016), but this was not possible due to scheduling clashes and pandemic-safety concerns. To offset this, the interviews were conducted via phone or web conferencing. For confidentiality reasons, audio was stored and used during transcription and volunteers were referenced as participants during recordings.

Delimitations

Delimitations are the bounds and scope of a study resulting from the exclusionary or inclusionary choices of the researcher (Simon & Goes, 2013). Research delimitations enable researchers to limit the scope and variables of their research study (Marshall &

Rossman, 2016; Theofanidis & Fountouki, 2018). Exclusionary delimitations included privacy practitioners—consultants and SMB leaders/agents who did not meet all the criteria. My study was limited by the selection of two groups of privacy practitioners—consultants (P1C) and C-suite business leaders (P1Cs and P2Cs) of small and midsized companies located in the Mid-Atlantic United States who had successfully safeguarded employee privacy. I used the multiple case study to explore and compare their privacy safeguarding strategies. Other details such as age, gender, midlevel managers, frontline employees, consumer, and applicants' perspectives were excluded and left for future studies.

Significance of the Study

The findings from my study identified strategies that small business leaders use to safeguard employee privacy. These strategies and derivative processes may result in reduced employee stress, enhanced creativity, and innovation, mitigating the risk of informational injury and legal costs and supporting a sustainable business that benefits employees, families, and communities.

Contributions to Business Practice

The findings from my qualitative multiple case study on strategies for safeguarding employee privacy identified opportunities for enhancing leadership and organizational capabilities that may reduce sometimes costly privacy invasions and intrusions. The findings of my study may equip business leaders with capabilities to reduce the costs and risks associated with employee/workplace privacy concerns and infractions as well as personal information injury, and by extension may reduce exposure during organizational sabotage or breaches. The findings from my qualitative multiple case study offer more in-depth insight into the management of risks associated with employee/workplace privacy and thereby support business viability.

Implications for Social Change

The findings of my study may be used or adapted to inform organizational policies, strategies, programs, and procedures in support of the human right of privacy, per Article 12 of the United Nations Universal Declaration of Human Rights (Claiming Human Rights, 2018). The findings may also equip business leaders with successful strategies that can be operationalized to safeguard employee privacy and support organizational longevity. When businesses endure, their leaders may contribute to employment opportunities for community members and facilitate economic resilience for their families and their communities (Edwards-Brown, 2020). The findings may also encourage trusting employer–employee relationships that promote employee well-being, which is beneficial for both families and communities.

A Review of the Professional and Academic Literature

The purpose of this qualitative study was to explore the CT and CL constructs used by privacy practitioners of SMBs in safeguarding employee privacy. A critical analysis and synthesis of the literature provided the context and blended theoretical framework for the research relating to complexity tenets and CL constructs and their application in the organizational field of SMBs. The literature review was foundational for understanding the phenomena both within and surrounding the safeguarding of employee privacy in SMBs. In addition, the intent of the literature review was to identify knowledge gaps for justification of the study (Saunders et al., 2019). This literature review highlighted gaps in the knowledge of privacy strategies and needs of employers and employees in U.S.-based SMBs.

This literature review consists of the opening narrative and discussions of its application to the business problem and conceptual framework. The selected literature included both quantitative and qualitative research studies and related papers. The primary databases used in this literature review included ProQuest, ABI/INFORM Global, and Walden University online library resources and Google Scholar. Key search terms for conducting research for the literature review included *complexity*, *complexity leadership theory*, *privacy by design*, *small businesses*, *privacy*, *workplace privacy*, *surveillance technologies*, *employee privacy*, *informational injury*, *personally identifiable information (PII)*, *sensitive information*, *health information*, *privacy preserving*, and *privacy enhancing.*

I used the Ulrichsweb global serials directory database engine to validate the peer-reviewed and scholarly reference listings. Additionally, if an entry was not listed in Ulrichsweb search engine results, I used the journals' homepages to perform the needed validation for inclusion. Table 1 summarizes, lists, and numerates the references, of which at least 85% were published within 5 years of chief academic officer (CAO) approval; the total number of references that were peer reviewed; and the percentages of peer-reviewed journals and scholarly references.

Table 1

Source*s of Data for Literature Review*

Literature review sources characteristics			
	Total	Number within 5 years of expected 2022 graduation year	Percentage (within 5 years of 2022)
Peer-reviewed journals	75	72	96.00 %
Other	43	32	74.41 %
Total	118	104	88.15 %

The review also included a critical analysis of supporting and contrasting conceptual models and themes for CT, CL, and workplace privacy. The review is divided into subsections addressing the following topics: (a) complexity and CLT, (b) alternatives to complexity frameworks, (c) CT, (d) the CL framework, (e) limitations of CL, (f) CL and administration leadership, (g) CL and adaptive leadership, (h) CL and action-centered leadership, (i) CL and chaos, (j) CL in the knowledge era, (k) CL and decision making in complex adaptive systems, (l) CL and privacy, (m) employee/workplace privacy and organizational design, (n) employee privacy and organizational actors, (o) employee privacy and organizational privacy programs, (p) ensuring employee privacy by design, (q) employee privacy and the internet, (r) employee privacy and the Internet of Things (IOT), (s) employee privacy and Big Data, (t) employee privacy and working from home, (u) employee privacy and surveillance technologies, (v) employee privacy and security, and (w) CL and employee/workplace privacy.

Complexity and Complexity Leadership Framework Theory

The composite conceptual framework I that chose for my study was CT and CLT. Complexity has not been formally defined, except in a metaphorical manner against natural occurrences in various hard scientific fields such as biology, chemistry, and physics, to name a few (Rosenhead et al., 2019; Zimmerman et al., 2008). However, complexity science provides a lens through which organizations are viewed as complex systems that respond to their environment and that cannot be observed using traditional linear methodologies (Schneider et al., 2017; Turner & Baker, 2019). During the 1990s, researchers extended and adopted CT into the social sciences and then applied CT to organizational leadership and processes (Uhl-Bien, 2021). Researchers use CT as a bridge between the natural and social sciences to view organizations as complex adaptive systems.

The acceptable application of CT in the social sciences has been debated by researchers. When CT has been applied to the social sciences, organizational science, and organizational leadership, CT has been purported to be able to cope with stable and unstable-chaordic experiences, enabling, administrative, and adaptive capabilities of both the enterprise resources and the leaders thereof (Rosenhead et al., 2019). However, some researchers have argued that these claims are unsubstantiated and result in quasi-science interpretations of phenomena. Yet, some researchers are stating that these claims are possible even without the underlying interactions of the scientific method. Rosenhead et al. (2019) stated that CT purists have concluded that the field of complexity theory is concerned with the behavior within certain types of systems over time. This conclusion suggests that some systems are outside the scope of complexity applications.

In contrast, some researchers see complexity as a complementary tool for the portfolio used to understand various experiences as systems in various contexts. As such, some researchers have noted that complexity sciences illuminate the success of the past, reflect an appreciation for cross-disciplinary interactions, are built on patterns that may be thousands of years old, and reframe perspectives on many systems that were partially understood or neglected by traditional Newtonian bounds of science (Zimmerman et al., 2008). These interpretations allow for complexity sciences to approximate understandings beyond Newtonian bounds.

Alternatives to Complexity Frameworks

I did not choose general systems theory (GST) for my study. GST approaches systems problems within stated boundaries (Turner & Baker, 2019). GST is more easily applicable to nonsocial systems, where the human element does not penetrate the determined boundary. Transactional systems may be approached with this theory, but social systems illuminate the limitations of hard boundaries and cannot account for the emergence of new order within the current system. As such, GST was determined not to be a fit for my study.

Complexity Sciences/Theory

CT has key constructs and guiding principles. Key constructs underlying CT are (a) an amalgamation of various theories, (b) the butterfly effect, (c) fractals, (d) nonlinearity, and (e) a view of organizations as complex adaptive systems. Guiding principles of CT are (a) clockware versus swarmware, (b) wicked questions, (c) nonlinearity, (d) interconnectedness, (e) diverse, (f) learning—intuitive and known knowledge, and (g) emergence (Zimmerman et al., 2008). Practitioners using CT have suggested the following principles:

1. Complexity view of the system—combine mechanical and biological
2. Build a good-enough vision—minimum specifications
3. During uncertain periods, lead with clockware and swarmware in tandem
4. Tune your place to the edge
5. Listen to the shadow system
6. Uncover and work with paradox and tension
7. Go for multiple actions at the fringes; let direction arise
8. Grow complex systems by chunking
9. Mix cooperation and competition (Zimmerman et al., 2008)

Even though complexity science is relatively new, practitioners and observers of its constructs and principles have facilitated its application in organizational and leadership arenas.

Complexity Leadership Framework

The CL framework supports mindset and behavior models to guide organizational decision making and sensemaking on individual and organizational levels. Correspondingly, CLT provides powerful, flexible mental models for developing strategies to guide organizational inquiry and adaptive responses to changing business conditions (Hazy & Prottas, 2018; Zimmerman et al., 2008). The CL framework proposed by Marion and Uhl-Bien in 2001 includes adaptive, generative, administrative, and enabling leadership theories (Hazy & Prottas, 2018). According to Uhl-Bien, CLT addresses all Rost’s 1993 typology for leadership—the nature of leadership as relational; the peripheral elements; leadership for individual and organizational adaptability; and “content”-complexity leadership mindsets, behaviors, and styles. CL involves appreciation for the nature and behaviors of the agents of change in any capacity—leader or follower—and mindfully uses levers to craft relevant adaptive responses. CLT encompasses leadership as a multilayered, dynamic system of collaboration and coordination; as acts of spontaneous, bottom-up, emergent responses; and as continuous acts of relational and connected accomplishments.

CL has evolved from the natural sciences, and its characteristics have been used by contemporary researchers to explain or interpret various organizational phenomena. CL was extracted from the natural sciences and adopted in the 1990s into the social sciences by researchers such as Uhl-Bien, Marion and McKelvey, in 2007,   who extended the theory into organizational processes (Rosenhead et al., 2019; Uhl-Bien, 2021). Some researchers view CL as a change model of leadership that helps leaders to tap into the informal dynamics within an organization as part of the process of designing robust, dynamically adapting organizations (Rosenhead et al., 2019; Turner & Baker, 2019). The CL framework involves considering the small effects, among many networked agents, even at the microlevel, that can eventually bring about macrolevel organizational adaptations.

CLT has key constructs related to networked interactions and emergence and can be used to present close approximations of phenomena. Key constructs underlying CLT are (a) the interaction dynamics among multiple networked agents and (b) how emergent events—such as creativity, learning, or adaptability—arise from these interactions (Uhl-Bien, 2021). According to Brown (2011), CL facilitates a subjective, plural, social autopoiesis view of a phenomenon (Hieker & Pringle, 2021). CL scholars have posited that knowledge is derived from within individuals and from interactions between agents and their networks. Knowledge is not only driven into a system, but also may also emerge from within a system as a program of action (POA). Moreover, knowledge is not developed or distributed via hierarchies. Finally, the adoption and application of knowledge are of paramount importance to organizational development (Cheng et al., 2020; Doyle, 2019; Uhl-Bien, 2021). These tenets support the interpretation of a variety of organizational products and even attempt to explain how they emerged.

I selected the CL framework instead of transformational leadership (TL). TL is a type of role-based leadership that inspires change in employees and an organization due to a push from leaders (Asbari, 2020; Benmira & Agboolah, 2021; Safonov et al., 2018). Alternatively, CL is a form of shared leadership that is reflected by five leadership/actor/agent functions that support adaptation: generative, administrative, community building, information gathering, and information using (Simpson, 2018; Uhl-Bien, 2021). With TL, change occurs due to the motivational and inspirational capabilities of a leader figure. However, the TL concept stops short of explaining or describing emergent leadership phenomena. TL also does not address the heterogenous capability of an organization and its ability to self-organize and be self-producing, as illustrated by complex adaptive systems of businesses.

Another familiar approach for organizational research is total quality management (TQM). TQM is a teamwork practice used to make businesses as competitive as possible, while fulfilling an organization’s potential, by trying to improve the worth of the products produced, the services rendered, the people employed, the processes created, and the environments established, with a focus on customer expectations and satisfaction (Marchiori & Mendes, 2018). TQM does not allow for swarmware activities, which are emergent and may even result in some chaordic episodes that CT facilitates and expects.

Another familiar approach for leadership in organizations is transactional leadership (TL). Transactional leadership focuses on hierarchical authority to motivate people. Carrot-and-stick methods with clear policies and expectations are incorporated by leadership to galvanize employees (Benmira & Agboolah, 2021). TL works best in clockware experiences, which are events that are outputs of established processes and policies. The dynamic, agentic, adaptive, emergent possibilities of CL may not be recognized or valued in this framework.

Comparatively, CL considers the value of all stakeholders and captures the emergent phenomena that establish value for organizational development and sustainability. CL affords a whole organization view to bring about solutions designed through shared leadership and followership adoption to support the development of the organization (Lester et al., 2017; Lorinkova & Bartol, 2021; Uhl-Bien, 2021). Organizations are nonlinear and dynamic, meaning that they are multifaceted, always changing, and not always controllable or predictable—a mixture of clockware and swarmware activities (Doyle, 2017; Hazy & Prottas, 2018; Turner & Baker, 2019; Zimmerman, 2008). CL provides a robust and practical framework for the chaordic experiences that are more evident in this volatile, chaotic, and uncertain period.

Any organizational analysis without consideration for networks, culture, and the climate of the organization could result in suboptimal solutions being presented. Leaders could anticipate emerging needs and facilitate a context and interactions that produce valued organizational processes (Coss & Dhillon, 2019; Uhl-Bien, 2021). CLT is nested in the idea of complex systems theory. Complex systems theory focuses on continuous learning, scanning, and the mental agility and acuity of the organizers participating in a social networked relationship (Baltaci & Balcı, 2018). As such, this theory presents key criteria for success in the organizational development and sustainability of SMBs, as it addresses the underlying microdynamics that result in new ordering of an enterprise. Leaders of SMBs could therefore engage the adaptive, emergent levers and hybrid philosophy of complexity theory to engage multi-actors to develop value-focused decisions to overcome traditional known challenges and to face the dynamics of the unknown.

As such, the use of CT and CLT could provide a dynamic, collective perspective on the participating organizations' strategies for safeguarding employees' privacy in support of organizational development and longevity. By using this composite lens, I sought to gain diverse perspectives and gather rich data for a deep understanding of the employee privacy strategies used by participating SMBs. I therefore did not use TQM or transactional leadership theories but used the composite lens of CT and CLT to identify and explore the strategies that SMB leaders, as privacy practitioners, used for safeguarding employee privacy.

Limitations of Complexity Leadership

CL emerged as researchers and practitioners wrestled with the inadequacies of the classical philosophies to organizational management, development, and leadership, in the knowledge era. To many, CL is a needed upgrade to leadership theory to reflect our shift out of the third Industrial Era (Uhl-Bien, 2021). Yet, even during the knowledge era, the limitations of CL have been noted by scholars. CL has not been able to answer all dimensions of organizational power dynamics, reduce the focus on heroic leaders, promote vertical development of actors, nor does it consider the amalgamation of holons and the within and without the self.

CL has some limitations, in explaining power dynamics in the organization and collective bargaining relevance. Researchers also, propose that CL should not rely on individuals since this is a duplication of organizational success theories. CL does not reflect the tenets of integral and vertical leadership frameworks. CL is limited in explaining and discussing power relations and union labor process (Baltaci & Balci, 2018). Also, according to Tourish (2019), CL should not focus on contriving heroic leader agency or leadership, and attribute solutions to an individual, but engage the communication and process systems levers to unravel the organizational entanglements. CL does not focus on the internal vertical development of the leaders and their various stages of development and how their mindset relates to choices, decisions and the organizational pathway and culture. The vertical development leadership layer proposed by Barret Brown in 2011, as meta-integral leadership with its 8 action logic levels (Hieker & Pringle, 2021) is left out of the current CL model. CL also does not address

Ken Wilber’s (2000), all quadrants, all levels (AQALS) integral leadership framework which examines leaders and leadership from both within and without the self – and its developmental stages, in tangent with the external environment, from an amalgamation of many fields of study (Rant, 2020). CL stops short of the complexity of the leader persona and mainly addresses the complexity of the external environment and the needed capabilities of adaptation, administration and enabling for learning and innovating, to meet these challenges.

However, the limitations of CL do not prohibit its use as a lens for this study. The limitations delineate the aspects that would not be covered by this study. CL will be used to explore the organizational event of safeguarding employee privacy with consideration for the limitations noted by above, pertaining to centrally controlled power relations and labor process - collective bargaining and labor unions. The locus of leadership is beyond roles, and in isolation, to unearthing contextual interactions across a whole social system (Ospina et al., 2020). Therefore, in this study, leadership is not role based and is a result of network interactions.

CL is a fusion of leadership considerations. CL is a hybrid of hierarchical, adaptive, and action-centered leadership capabilities (Baltaci & Balcı, 2018). On the one hand, CL requires a defined profile of the organization that allows for ease of access for changing administrative actions whilst the creative problem solving and continuous learning dynamics that emerge from the co-creative interaction of the social networks reflects the adaptive and generative aspects (Uhl-Bien, 2021). The use of effective decision-making mechanisms for responses during operational and crisis events, is indicative of this action-centered leadership.

Complexity Leadership and Administration Leadership

CL supports the use of many other management areas. The administrative aspect of CL is based on strict control and a significant bureaucratic hierarchy (Baltaci & Balci, 2018). Complexity practitioners are aware of the duality of an organization. *Clockware* activity (Zimmerman, 2008) such as administrative tasks in support of current organizational design are a capability SMBs should hone. For instance, on the dimension of information privacy, Cha et al. (2019) suggested using high-level principles of general data protection regulations and the International Organization for Standardization (ISO)/International ElectroTechnical Commision (IEC) 29100:2011 requirements to produce an actual resolution for such privacy threats in the organizational Internet of things (IoT) ecosystem. Rath and Kumar (2021) have suggested that information privacy be considered at the individual, group, organizational and societal levels. As such, SMB leaders should be aware of the implications of privacy invasions on their individuals, groups and the organization and society.

Complexity thinkers in the SMBs may incorporate aspects of various theories and apply them to the organizational context. For instance, SMB leaders could incorporate theories such as communication privacy management theory (CPM), Privacy by Design (PbD), Business & Human Resource (B&HR) and generative emergence. CPM considers privacy turbulence, boundaries, network member responsibilities, and established rules for sharing information (Smith & Brunner, 2017), whilst strategic PbD (Cronk, 2018) considers the engineering principles purported by Cavoukian, in 2017 (Cavoukian & Chibba, 2018) and Business & Human Resources (B&HR) discussed by Egert et al., (2021) suggested that the privacy solution should be human centered. Through the lens of complexity theory, and an appreciation for generative emergence, SMB leaders could develop and implement policies that reflect the valuing of employee privacy.

Employee privacy is complex notion. According to Gerlich et al., (2022), the privacy ecoscape is made up of short term, transactional interpretations of privacy concerns, as reflected in the privacy calculus concept and the long term and intrinsic, always developing interpretations such as Multi-Dimensional Privacy Theory (MDT) which supports a more complex and comprehensive appreciation of the employee privacy phenomenon. The privacy calculi notion posits that individuals weigh the benefits and risks of disclosing personal information against the benefits of those exchanges (Gerlich et al., 2022). As such, SMB leaders/agents could incorporate privacy concerns not only as they pertain to the various privacy calculi, but also with an understanding that employee privacy concerns are the result of their environment, interpersonal interaction, and individual experiences.

The idea of an economic privacy perspective, such that data subjects are enlightened and aware of what the exchanges require, is not true as evidenced by the quiet, unagreed upon, privacy invasions by corporations in the United States of America. The Cambridge Analytica fiasco, and many other impingements on citizen privacy have revealed the unscrupulous patterns of an Orwellian dystopia. As such, employee privacy as a reasonable expectation at work is paramount (Bhave et al., 2020). An amalgamation of various theories could be considered in the development of employee data privacy governance strategies - a service line item of which is safeguarding employee privacy using policies, processes, personnel, tools, techniques, and other resources to effectively and efficiently, deploy it.

Complexity Leadership and Adaptative Leadership

The COVID 19 pandemic environment reflects the need for addressing adaptive issues related to workplace privacy. Concerns and needed resolutions around the use of surveillance technologies which may allow for informed control, new ideas of organizational controllability, employee privacy limitations, work design, trust, and employee-employer relations, are being revisited (Uhl-Bien, 2021; Katsabian, 2020). The adaptive aspect of CL is fundamentally based on engaging entrepreneurial leadership, creative problem solving, resonating with new conditions, and learning to create adaptive solutions. (Balataci & Balci, 2018; Uhl-Bien, 2021). An adaptive challenge rattles an organization to its core. The reverberations are far reaching, and if left unmanned could result in the implosion of an enterprise.

Leaders of SMBs need to have the capability to anticipate and respond to changing expectations of their various stakeholders and environment. They should also understand that informal activities may result in *swarmware* behaviors that support emergent change (Doyle, 2019; Zimmerman, 2008). Enabling leaders must amplify and scale emergence across the system by navigating the adaptive tensions through the adaptive space (Uhl-Bien, 2021). As such, the leaders of SMBs need to engage the appropriate frameworks, models, tools, and strategies to safeguard workplace privacy along the dimensions of personal information, environment, and autonomy.

The COVID 19 pandemic amplifies the need for the capability to safeguard employee privacy in a distributed design. With approximately 62% of the American workforce switching to teleworking due to the COVID 19 Pandemic, there have been many new implications for privacy (Katsabian, 2020). This hybrid occurrence provokes employers to re-examine the balancing of the needed levels of surveillance for business needs with privacy of their work from home employees, as well, as the traditional work design constructs (Katsabian, 2020). Under the pandemic environment - home-office engagements moved the boundaries of reasonable expectation of employee privacy, into the forefront.

Complexity Leadership and Action-Centered Leadership

This action-centered leadership aspect suggests that leaders of SMBs scan current environments, anticipate threats and ways to treat risks and design solutions – i.e., people, finances, technologies, policies, and processes to support a sustainable future view. According to Balataci and Balci (2018), the action-centered leadership of CL is displayed when decision mechanisms function during crises and dynamic capabilities events. Complexity practitioners enable learning and co-evolution by cultivating an organizational climate and culture that supports such outcomes (Smith & Brunner, 2017). Furthermore, enabling leaders appreciate complexity, value being present, observing and reacting in the moment, and leverage the tensions between the formal and informal organization, to infuse complex adaptive systems (CAS) with learning, adaptive and creativity capabilities (Backlander, 2019; Uhl-Bien, 2021; Wheatley, 2011). The action centered leadership aspect of CL facilitates dynamic capabilities for adaptation.

Complexity Leadership and Chaos

I used CL to explore the safeguarding of employee privacy, as a communal activity, within a context of volatile, chaotic environments and complex social systems. CL practitioners accept and leverage non-linearity, indeterminacy, uncertainty, and the distribution of power and influencers in their organizations (Tourish, 2019; Uhl-Bien, 2021). The use of ubiquitous, cloud computing capabilities from interconnected technologies to perform surveillance on various populations, such as consumers and employees, the onslaught of breaches, and the rise of the personal data market, and the blurring of physical work environments with digital workspace through new work designs, have created the perfect storm for a revisiting of employee privacy and organizational leadership (Bhave et al., 2020; Katsabian, 2020; Zuboff, 2019). This confluence of events provides ample opportunities for workplace privacy investigation.

CL considers the dynamic nature of an organization and the self-organizing capabilities of personnel to solve familiar and emergent problems. Key constructs underlying CLT are (1) the interaction dynamics amongst multiple, networked agents, and (2) how emergent events – such as creativity, learning, or adaptability – arise from these interactions (Uhl-Bien, 2021). An underpinning of CL is the dynamic capabilities framework based on the premise that capabilities not only vary across business enterprises, but the differences are the result of management choices (Scarpenelli et al., 2020). In other words, dynamic refers to the capacity to reconfigure the firm’s resources and processes to adapt to changing business environments, and capabilities refer to the strategic management of firm's assets to seize opportunities and sustain a competitive advantage (Scarpenelli et al., 2020). The COVID 19 pandemic presented ample chaos from which many small and midsized organizations may have adapted their approach to the safeguarding of employee privacy.

Secondly, the focus on micro-strategic leadership actions across organizational boundaries and levels, and an acceptance that outcomes are the result of complex interactions. Also, CL illuminates the relational foundations of change in emerging organizational fields and supports the formation of new social objects and a co-created social identity (Lichtenstein, 2020; Uhl-Bien, 2021). CL was used to explore the safeguarding of employee privacy efforts, with an appreciation for the volatile, chaotic, and uncertain context and based upon the premise that organizational meaning-making systems – (value-focus and sense-making), support self-organizing and emergent change of privacy-friendly processes, structures and offerings which can occur in complex social systems (Cheng et al., 2020; Sengupta, 2019; Smith & Brunner, 2017; Turner & Baker, 2019). This dynamic occurs because of the *informing* that occurs out of tensions among interacting agents (Lichtenstein, 2020). These unselfish interacting events illuminate the constructive process of collective actions and actors (Kay et al., 2018). CL, therefore, presented a lens to view organizational known or emergent problems with the collaboration of the networks' actors.

Organizational researchers have been grappling with the dialogic nature of organizational experiences. One of the topics under investigation is that of the appropriateness of CL to the practice of organizational management (Tourish, 2019). CL is responsive to non-linearity and unpredictability, but strong communication and process perspectives would cater to these vacillations (Tourish, 2019). As a matter of fact, CL posits that leaders should be able to orchestrate many skills, navigate the ambidextrous organizational requirements, be aware of the internal and external environment, adapt, learn, and create (Uhl-Bien & Arena, 2018). Business leaders should be able to think broader, embrace the dynamic nature of organizational experiences, and interactively organize (Uhl-Bien, 2021). Business leaders, as actors, should appreciate the co-creative efforts at play within their complex adaptive systems and surrender to new ways of knowing and sensing to be sustainable.

Adaptive competency is paramount in this era of chaordic acceptance. The chaordic behavior of business environments, has supported the need for capabilities that can straddle current operations, while attending to emergent issues and problems (Kay et al., 2018; Pappas, et al., 2018). In fact, the ability of business leaders to integrate, build, and reconfigure internal and external competencies to address rapidly, emerging change environments, is now crucial to organizational longevity (Kay et. al., 2018, Uhl-Bien, 2021). The capacity of CL to refer to practices and processes, as opposed to roles and responsibilities, makes it a good theory for exploring the interdependencies of the many actors across the enterprise network that collaborate to deal with complex problems (Craps et. al., 2019). From the relational perspective, leadership emerges from the interactions among persons, groups, and organizations (Uhl-Bien, 2021). Further, contemporary discussions, in the era of complexity and chaos, have been moved towards plural pragmatic interpretations, and appreciations of the new co-created reality which Lichtenstein, in 2016 stated, emerges when actors/leader/agents use their personal agency to create the needed conditions from which something new can emerge and eventually co-create a new order (Uhl-Bien, 2021). CL may be used to map relationships both within and outside the firm. SMB leaders could leverage this self-correcting communal capability to arrive at solutions that safeguard employee privacy.

Complexity Leadership in the Knowledge Era

The Knowledge Era is characterized by the forces of globalization, technology, digitization, deregulation, and democratization, collectively creating a new competitive landscape. The knowledge era identified the various knowledge sets that could be captured with the advent of the internet and personal computing (Uhl-Bien, 2021). Surveillance technologies may be used to monitor cyberloafing behaviors and information incident management. However, researchers have also identified some serendipitous side effects in the relationships between internet employee usage policy satisfaction, intrinsic work motivation and how much an employee wants to stay with an organization (Jiang et al., 2022). With the ascension of connected, pervasive, surveillance and learning technologies, the Digital Era has realized the capturing of various personal knowledge sets - related to workspace (environmental), personal information, and mental intrusions/invasions (autonomy).

The CL framework considers the chaordic events that can occur during organizational development. In the current competitive environment, learning and innovation are vital for competitive advantage (Uhl-Bien, 2021), and emerge due to *swarmware* activities instead of solely mechanistic tactics for control which are being proven to not be beneficial. Researchers have proposed CL as a framework for leadership, in the fast-paced, volatile, and uncertain context of the Knowledge Era, and as a needed upgrade to leadership theory, to reflect our shift out of the Industrial Era (Uhl-Bien, 2021). Through the CL lens, effective leadership does not reside exclusively within the leader's symbolic, motivational, or charismatic actions, and SMB actor/agents/leaders may assume that change events occur because of organizational learning and innovative activities, which result from interactions.

SMB leaders, as organizational actors, must be able to forget, unlearn and embrace the dissonance that comes with disruptions of known processes and behaviors. CLT focuses on enabling the learning, creative, and adaptive capacity of complex adaptive systems (CAS) that produce organizational knowledge (Uhl-Bien, 2021). CL is a change model of leadership that helps leaders to tap into the informal dynamics of generative emergence within an organization as part of the process of designing robust, dynamically adapting organizations (Uhl-Bien, 2021). CL focuses on the complexities in complex adaptive systems and entanglements that make up an organization.

Complexity Leadership and Decision Making in Complex Adaptive Systems

A challenge of CL is to effectively tap into the entanglement between the administrative *(clockware)* and adaptive structures and behaviors (*swarmware)*. Keeney's value focused policies, procedures and processes support and sustain organizational development (Coss & Dhillon, 2019; Poleto et al., 2020). Organizations that function as complex adaptive systems (CAS) have many actors that exchange information, mutually affect each other, and, in so doing, generate new valuing of behavior in specific areas that affect the system (Bryson et al., 2017; Horvat & Filipovic, 2018, Uhl-Bien, 2021). SMB leaders/agents could link the two organizational behaviors of *swarmware* and *clockware* activities through their decision to value employee privacy, and thereby implement policies, procedures, and processes, to that end.

SMB leaders who practice value-focused thinking and make privacy related decisions, can unearth information, environment, and autonomy privacy objectives. Their decisions should not only be based on the socio-technological precepts and principles, regulations, standards and legislation, the values of individuals within the organization, but with a collective human-centered valuing of privacy, as a universal principle, and a human right and need (Coss & Dhillon, 2019; Ebert et al., 2021). SMB leaders/agents could view autonomy as socially embedded, and the single most important element for creating employee engagement, commitment, and well-being, which yields creativity and innovation (Burcharth et al., 2017; Mankins & Gortar, 2017; Mokrosinska, 2018; Sarmah et al., 2022). These leaders could note the intrinsic value of privacy since it is essential and instrumental for thinking and acting freely-autonomy. However, unchecked autonomy could lead to organizational chaos. To mitigate chaos, SMB leaders could:

1. Balance autonomy with accountability through *clockware* administering activities that provide strategies, tactics, feedback mechanisms for quality management, ownership, and appropriate responses for addressing both success and failure to reach predetermined goals. Establish clear line of sight

objectives, appropriate work design and controlled leadership that support collaborative and individual contributions.

2. Balance *swarmware* and *clockware* activities through the mechanism of culture. Ambidexterity in leaders/agents is a needed competency. Mapping the relevant activities to the various areas of the enterprise is necessary to optimize this strategy.
3. Facilitate the coordination of various empowered autonomous teams that can easily respond to changes, for instance, in regulations, the economic environment, and data subjects' awareness. (Mankins & Gortar, 2017).

Heightened privacy awareness suggests that business leaders may respond with care and transparency to re-establish trust. Transparency may be defined as - process visibility, information disclosure (benefits) - transparency facilitates organizational learning, innovation, communication, and collaboration (Gierlich-Joas et al., 2022). To harmonize privacy with transparency, SMB leaders/agents could revisit the privacy-transparency paradox and develop new ways of designing for the privacy concerns of their employees and the accountability needs of the enterprise.

SMB leaders/agents may harmonize the tension between transparency and accountability needs of their organizations through various tactics. According to Gierlich-Joas et al. (2022) to erase the tensions between transparency and employee privacy needs SMB leaders/agents could:

1. Create zones of Privacy

2. For the personal sphere - an employee’s valuation of privacy needs to be understood - individual privacy preferences can be met in the workplace.
3. For the interpersonal sphere - agents could triage information data sets and only disclose on a need-to-know basis to allow for information privacy – Group of stakeholders with co-ownership of information data sets could be trained and organizational boundaries, policies for exchange, disclosure, storage should be established.
4. For the environmental sphere - responsibility for employees’ privacy could be heightened and a specific role could be developed. SMB leaders/agents could also determine whether digital solution providers should be held responsible for incorporating privacy-by-design measures. Agents could also co-develop measures to reduce their employees’ privacy concerns. Companies need to evaluate the value of privacy for their business models.

There are new ways of thinking and designing of an organization that can support the valuing of employee privacy during this digital data deluge. Business leaders could be crafting socially responsible enterprises that thrive and go beyond the systems focus of traditional sustainability efforts, and into respect for planetary boundaries and humanity (Beehner, 2019). Clearly, in the poorly regulated U.S. digital economy, characterized by pervasive surveillance technologies, big data analytics, internet of things, and artificial intelligence under the guise of freeness, ease of use and access to information, nefarious patterns (Cronk, 2018) have resulted in attacks on democracy and privacy through the iniquitous restructuring of industries and markets, that impede free market traditional behaviors, the stripping and monetizing of personally identifiable information, the blurring of workplace privacy boundaries and the establishment of surveillance capitalism (Cavoukian & Chibba 2018; Katsabian, 2020; Zuboff, 2021). SMB leaders/ agents could protect and secure their market contexts and governance framework, by attending to the valuing of employee privacy.

The equilibrium of selfinterest and morality may be pursued by contemporary leaders, and business owners may recognize employee privacy, as a moral human right and need, and craft solutions that safeguard it. The perceived loss of privacy affects a person's independence, integrity, and dignity (Bloustein, 2018). There may be a moral value in the capitalistic behaviors of business leaders and an understanding that privacy is both a human right and need (Voss, 2017). Dhillon et al. (2018) suggested that following a strategic decision analysis perspective, values can be converted to objectives, whereby the objectives focus on prevention. As such, contemporary business leaders/agents should value privacy as a cornerstone for the wellness of their employees since this value objective may result in positive effects on retention and productivity.

Having a well-honed sense-making capability makes it possible for SMB leaders/actors to develop privacy safeguarding solutions that are relevant and effective. For this knowledge/digital era, business leaders need new ways of knowing, sensing, interpreting, and engaging to lead successfully, beyond role-based influence, in complex environments (Uhl-Bien, 2021). The business leader would need to balance their business needs for monitoring, with their responsibility to safeguard the human right and need of employee privacy.

Complexity Leadership, and Privacy

Scholars across the fields of law, technology, business, and sociology have presented privacy in many ways. There is high complexity and scope of workplace privacy (Teebken, 2021). Some thinkers posit that it is dead, since the divide between an employee's personal life and employee status is diminishing, due to social media exposures and linkages to hiring and promoting, and corporate employee email, website behaviors and location monitoring, available due to the use of Bring Your Own Device practices (BYOD). Privacy is being eroded by technocrats, who respond to the uncovering of their nefarious harvesting acts, by suggesting regulations and policies that congress should enact (Boatwright et al., 2020). Privacy is not yet dead as a cultural concern (Igo, 2022). Is it possible that our understanding of privacy should not be based only on a user perspective? The notion of privacy goes beyond technology dimensions.

Through the years scholars have identified privacy harms such as mental distress, embarrassment, reputational impact, resulting from invasions on physical distancing, secrecy, and the right to be left alone. Contemporary thinkers on privacy, who view privacy within the Orwellian Big Brother capability, support conversations on Warren and Brandeis (1890) as privacy as a right to be left alone, Westin's 1968 secrecy paradigm, the right to be in a state of privacy, to have a safe space distance (Katsabian, 2019), the invasion conception by relational privacy researchers such as, Solove (2006), Nissabuam (2011) and Mokrosinska (2018). Privacy has also, been plainly stated as a universal right and need (Ebert et al., 2021). Privacy continues to play a key role in fostering autonomy, emotional health, self-evaluation, and protecting communication, and any shortcomings of traditionalist views should be re-imagined and if possible, augmented by new appreciations of the emergent needs in this interconnect era (Huppertz et al., 2020; Mokrosinska, 2018; Ruiner et al., 2022). These perspectives augment each other and move through the governance of the individual self, social-group privacy, political, and even economic discussions regarding privacy.

Sometimes the impetus for organizational changes comes from external forces – market dynamics, individual or societal norms. Righettini and Sbalchiero (2017) concluded that there may be external drivers of organizational changes that find their way into processes, policies, and programs. Organizational changes may also emerge from the dynamic entanglements of networked interactions, individual and collective dissonance – complex interactions, and create new values and ordering of the enterprise (Lichtenstein, 2020; Wheatley, 2017). The digital context has highlighted the criticality of privacy as a human right and need (European Union, 2018). The COVID 19 pandemic rapidly changed business models to distributed remote networks and drove the hybrid work from home model for many organizations.

The complexity of the notion of privacy, may be noted through the many interpretations and dimensions that all come with limitations due to legal and ethical acknowledgements and enforceability of ownership, invasions, and harms. In a recent survey on privacy conducted in the United States, 90% of the respondents stated that it was important to control information about themselves (Kshetri et al., 2020). Even though this survey highlighted information privacy, people can take a more defensive posture in the face of the current tenacious onslaught of surveillance capitalism which is dividing the notion of privacy into slivers, by which perpetrators and nefarious actors can abuse, misuse, and lobby to develop regulatory and organizational practices that do not address the whole concept of private affairs.

In this current era of digital predominance and remote work, the quest for knowledge along with pervasive surveillance technologies, it is probable that blurred lines between employer and employees may occur. The rise of the tensions of employees having digital profiles and employers using surveillance technologies not solely to monitor productivity, has highlighted the shortcoming of the many definitions of privacy that were a fit for days gone by (Bhave et al., 2020; Katsabian, 2019; Solove, 2004). The current distributed work from home context may result in many employees being over surveilled, due to the antagonistic perception between employee privacy and organizational needs. New ways of seeing these perceived tensions may be needed.

Thoughts on employee privacy need to reflect the considerations for this digital and knowledge seeking era. The pervasive, subtle, intricate network of the data collection bodies, their use, monetizing and sharing could result in a horrendous bureaucracy that can be hard to overcome by an individual. As such, Solove (2004) suggests that the notion of privacy be revisited in law, technology, and sociology, in this digital context. Ebert et al. (2021) suggested that the solution to this privacy dilemma requires a human-centered approach. A revisitation of the notion privacy, in law and business practices may lead to a newer societal adoption of the valuing of privacy as a human right and need, which can affect how and why we traffic and reveal private affairs.

Some scholars list personal information, environment, and autonomy as three dimensions of employee privacy. According to Smith et al. (2011) personal information privacy is the (perception of) control over the collection, use, and sharing of data sets on sensitive, health and personally identifiable information. Workspace privacy (environment) is the (perceptions of) control over the sensory stimuli (visual, space, acoustic, olfactory) in employees' work environment, and personal access. The environmental dimension also describes how individuals develop privacy concerns due to the impact of cultural, social, and physical settings. Autonomy privacy is the (perception of) control over one's self-determination and sources of volition (Gierlich-Joas et al., 2022). These proposed dimensions of employee privacy provide a realistic framework from which to analyze the impact of privacy invasions on employees. Business leaders/agents should recognize these dimensions and develop a culture that acknowledges them, to reduce risk and harms.

Privacy is a human right which should be safeguarded. In some scholarly circles, privacy is a protection of autonomy (Mokrosinska, 2018), while others view privacy as an economic asset (Walsh et al., 2017). Personal information privacy is the ability of a data subject to have control over information about oneself and it does not only encompass information that is explicitly shared, but also information that is generated implicitly (Choi et. al., 2017; Teebken & Hess 2021). Zuboff (2019) suggested that under this new regime of surveillance capitalism, higher privacy safeguarding considerations for the preservation of personal data is required. According to the US Federal Trade Commission (FTC) (2018), it is the responsibility of businesses to safeguard personal data. Privacy is a human right which should be guarded from nefarious patterns which can undermine autonomy, reshape markets and governance systems. Ignoring the privacy invasions can have effects on the self and society.

The complexity leader may be aware of the opportunities and threats of both self and the organization. The onslaught of reported abuses of personally identifiable information (PII) (Choi et. al., 2017), heightened by the advancements in technology, the internet, and the laissez-faire processing regulations in the US space, have raised the awareness of privacy rights and moved the conversation from regulators and corporations to the average citizen. Employees believe that their privacy is under threat (Bhave et al., 2020), whilst other groups state that privacy is dead (BBC, 2017: Mims, 2018). The heightened awareness of the implications of privacy invasions are now in the realm of the average citizen. The citizen response may be a tipping point to curtail these invasions of privacy,

Within this tension, new success factors may be emerging and may be incorporated into the information governance of an enterprise. Privacy awareness and heightened trust expectations are the results of robust discussions, on the role and responsibility of enterprises, on the human right of privacy declared in Article 12 of the United Nations Universal Declaration of Human Rights, 1948 (Claiming Human Rights, 2018). Dhillon et al. (2018) revealed ten privacy management objectives and suggested that organizations focus on trust and individual privacy protection. Valuing privacy as a human right and the incorporation of privacy management objectives, by business leader/ agents, may result in new organizational success factors being developed.

Small business leaders-actors/agents need to understand that with heightened privacy awareness comes different stakeholder expectations. As such, this could change how business leaders approach the governance of information privacy. Areheart and Roberts (2019) proposed that the Genetic Information Nondiscrimination Act (GINA) 2008, provided a basis for employee-privacy in the period of Big Data processing advocacy. Olteanu (2019) highlighted the significance of our genetic code as being our biological stamp which reveals our various predispositions to diseases. Olteanu (2019) and Areheart and Roberts (2019) suggested that GINA could be used to prevent employer breach of employee privacy, since big data analytics provide an opportunity to aggregate and cross-reference information, to gain access to some of our most intimate secrets, risks, choices, and personal relationships.

The separation between public and private spaces has been discussed in the western hemisphere. Igo, 2018, stated that privacy was discussed by Greek, British, and American philosophers. These philosophers delineated between the public spaces which can be accessed by government and private spaces that are based on self-regulation (Bhave et al., 2020). Our current dilemma in the US, is the lack of controls and delineation between these spaces by corporations.

Privacy as a human right and need has been undermined by the failings of the Federal Trade Commission (FTC) and is amplified by the power of the corporations to inform US consumer privacy policy, employee privacy and the abuses that stem from such deregulation. According to Fairclough (2016), the Fair Information Practices (FIPPS) of 1970's outlined eight principles for data security: 1) transparency, 2) purpose specification, 3) use limitation, 4) data minimization, 5) data accuracy, 6) individual participation, 7) security, and 8) accountability. Yet, the US regime only applied this to the responsibility of the Federal Government, to safeguard the privacy of federal employees. There has been a lack of understanding of individual's' perception of privacy in the workplace context (Teebken & Hess, 2021). Currently, private sector employees are without strong protections and subject to patchwork state laws.

Drivers of economic success and profitability in the SMBs, are affected not only by the value-focused strategies to have an objective privacy safeguarding program but may pursue a socio-technological solution and procure privacy ready technologies to meet the demands of the privacy aware stakeholders. Riveni et al. (2017) suggested that user awareness is the beginning of effective privacy controls within these systems. Ebert et al. (2021) contended that this socio-technological and individual perspective approaches are insufficient for the scale and pervasiveness of the privacy infringements that are rampant under surveillance capitalism. Privacy controls should be both technological and cultural.

Employee Privacy and Organizational Design

Given the onslaught of cyberattacks, malevolent patterns and abusive surveillance practices, the safeguarding of employee privacy should be a consideration of privacy-friendly organizational design. With the noted trend of cyberattacks and impingements on privacy that are symptomatic of this digital era, business leaders/agents may value privacy as human right and develop privacy-friendly business processes, technologies, and network infrastructure as a strategic effort for cultural adoption, in support of employee privacy (Anciaux et al., 2019). They may also design to minimize employees perceived intrusion of privacy within blurred boundaries during the work from home switch during events such as the COVID 19 pandemic.

Responses to privacy invasions and abuses need to be developed and implemented. SMB leaders may embed privacy by design (PbD) across business processes, technologies, and networks, as a sound response to the pervasive surveillance technologies and abuses of privacy (Cavoukian & Chibba 2018; Cronk 2018). To retrofit privacy, SMB leaders may need to determine the privacy impact of existing IT systems that they wish to add to the ecosystem. For this, business leaders may reach for Hoepman's (2018) eight privacy design strategies:1) minimize, 2) hide, 3) separate 4) aggregate 5) inform 6) control 7) enforce, and 8) demonstrate. This approach may be a work around for techno-regulatory constraints. According to Ebert et al. (2021) SMB leaders may also add employee privacy as a subset of the strategic human resource function, since socio-technological solutions, retrofitting and the current US legal regime have proven to be inadequate responses to the deluge of the monetizing of personal data and surveillance abuses, prevalent under the current surveillance capitalism. Placing a human-centered response to this deluge may provide the needed perspective to develop a robust response to this pervasive privacy invasion dilemma.

Employee Privacy and Organizational Actors

Leaders of SMBs could be proactive and demonstrate care through an integrated security and privacy design for the personal data of their employees. Organizational leaders (actors) may internalize and practice self-change (Voss, 2017) concurrent with the change needs of the enterprise, as a dynamic continuous process, by which stakeholders co-create business processes. Developing and implementing security strategies to protect their corporate and personal data of its various data subjects, is now a mandate (Cook, 2017). By taking on this challenge, SMB leaders may shift organizational ethical and behavioral boundaries, in support of the safeguarding of employee privacy.

Additionally, leaders (organizational actors) of SMBs could be accountable, responsible, and surrender their authority, in support of the privacy assurance for their employees, valuing it as a human right. To this end, there may be tactical applications of differential privacy which may be used in the small enterprise, to block or jigger processors-technologies, personnel who do not have the right or need to know, pertaining to the personal data of employees (Xianmang et al., 2018). SMB leaders, as complexity leaders focus on the spaces between the interactions of people, ideas, and the environment, and allocate spaces for tensions that may develop new ideas, opportunities that expand ethical and behavioral boundaries of the firm (Lichtenstein, 2020). This ability to straddle the known and unknowns, to co-create fresh solutions for various stakeholders, may be needed for the SMB leader of this era.

Employee Privacy and Organizational Privacy Programs

Designing and implementing an organizational privacy program which safeguards employee privacy may be a consideration for SMB leaders in this privacy aware period. The notion of control over one’s information, workspace and autonomy has been the underpinning of employee privacy discourse (Bhave, et al., 2020). The notion of workplace privacy is currently blurred due to the COVID 19 pandemic and resulting work designs. The remote work designs and now, the work from home design has security, corporate reputation, moral implications for the use of big data analytical, surveillance and IOT technologies for employee performance, monitoring, and selection (Adams, 2017; Agarwal et al., 2017; Katsabian, 2020). The designers for these new work models may consider the implications of privacy and be governed by employee privacy valuing tenets.

The remote work design does not have to undermine employee autonomy. In fact, in trusting, co-creating culture, employees may be productive and be retained due to affective organizational commitment, when autonomy is balanced with transparency for the overall well- being of the organization. Autonomy - being free of the control of others (Gierlich-Joas et al., 2022), is another underpinning of employee privacy, and it is also under review based on the COVID 19 pandemic response for work design. Concerns and needed resolutions around the use of surveillance technologies which may allow for informed control, new ideas of organizational controllability, employee privacy limitations, work design, trust, and employee-employer relations, are being revisited (Uhl-Bien, 2021; Katsabian, 2020). The loss of privacy due the misuse of surveillance technologies, to monitor employee performance, even within the employee home, could undermine free acting and thinking and have negative implications for creativity and innovation in an organization, and on the wellness of employees.

Human-centered privacy management programs may be needed in this digital era. Business leaders may design employee privacy programs with the notion of privacy as a human right and need (Ebert et al., 2021) and anticipate the malevolent patterns that can occur in this current digital era. Clear procedures should be in place for collecting, using, sharing, retaining, and disposing of the various personal data sets of employees (Katsabian, 2020). The privacy program may therefore be designed, established, verified, and validated to support this human right. To operationalize the safeguarding of employee privacy, SMB leaders may look at the International Organization for Standards (ISO) 27701:2019 which provides opportunities for privacy management within an information security management system. ISO 27701:2019 offers guidance for personal data controllers and considerations for their data subjects/rights owners-such as employees.

SMB leaders may develop a Privacy Information Management System (PIMS) which balances the security needs for business information (BI) assets, critical information assets and employee productivity reporting with employee privacy. Since privacy has the concerns related to self, one's information and one's decision to express information sets depending on settings and audience (Solove, 2004), then, employee privacy relates to personally identifiable, health and sensitive information sets which they may express differently in a variety of contexts. The responsibility of SMB leaders is to first demonstrate the valuing of employee privacy by allocating resources to govern such information sets and experiences.

Designing a considerate Privacy Information Management System (PIMS) is based on the valuing of the reasonable expectation of privacy by the SMB leaders. SMB leaders could be mindful of the employees' reasonable expectation of privacy during the various processes such as collection, storage, sharing/transferring and handling of personal information sets (Shipman & Watkins, 2019). To account for the personal information sets, Shipman and Watkins (2019) presented considerations of a robust PIMS:

1. Personal information should have limited access controls and be confidential
2. Employees value the availability of their personal information and would share it when it is advantageous or if there is a bonafide business need.
3. Personal information should be in a usable format
4. Not be used to the disadvantage of the employee
5. There is an expectation that the personal information exchanged would be treated properly
6. Processed in a manner that adheres to the six (6) principles of the 2018 European Union General Data Protection Regulation (GDPR).

Business leaders may use these considerations for designing and implementing safeguards for personal information sets.

Ensuring Employee Privacy by Design

For SMBs, strategic privacy by design should take root. Informational self-determination is the bedrock of data privacy and insisting on trust in technologies is a new mandate to secure innovation, autonomy, and democracy. Chibba and Cavoukian (2018) discussed the impingement of democracy and the pervasive surveillance of Inter Communication Technologies (ICT). The gross misuse, monetization, and vast exploitation of personal data, with accessible artificial intelligent analytic tools, in the name of the new surveillance capitalism growth mindset, has altered the value of the human right to privacy. The termination of an over-surveilled employee cost a company more than 500,000 USD for lost wages (Tomczak et al., 2018). Business leaders (actors) could value privacy as a human right and need, follow the measure of positive sum, established by Howard Raiffa, to frame solutions for meeting organizational and stakeholder goals (Ebert et al., 2021: Ury, 2017), utilize socio-technological solutions such as: privacy by design (PbD) and privacy enhancing technologies and security practices, for physical design and infrastructure (Cronk, 2018). Employees are desiring safe private spaces, opportunities to be without pervasive, invasive surveillance and the organizational safeguarding of their personal information.

Privacy awareness has been heightened due to the deluge of breaches and misuse of personal data which provided ample opportunities for conversations on the risks of Big Data, coupled with analytical capabilities through machine learning and artificial intelligence. Privacy by design (PbD) mandate is a recent phenomenon in the United States, even though privacy considerations were reflected in many federal sector-specific statutes and individual state statutes such as: the Privacy Act (1974), Fair Accurate Credit Transactions Act (2003), Health Insurance Portability and Accountability Act (1996)(HIPAA), The Family Educational Rights and Privacy Act (1974)(FERPA/SHERPA), e-Commerce Act (2002), and the new California Online Privacy Protection Act (2018)(COPPA). The rising tide of privacy awareness is moving conversations and expectations beyond the short comings governmental and regulatory designs.

Although previous research, by Westin (1996) had shown that employees were not too concerned about their personal information. By 2006, organizational researchers such as, Agle et al. examined the relationship of employee perceptions of information privacy in their work organizations and identified some important psychological and behavioral outcomes. Agle et al. (2006) presented a model which linked the management of information privacy to empowerment, and empowerment to creative performance and Organizational Citizenship Behaviors (OCBs). Today, in this age of surveillance and artificial intelligent analytic tools that are consistently being incorporated into the ecosystem, SMBs leaders/agents/actors should consider the effects that the mismanagement of personal information may have on the development of their organization. A robust strategic approach to employee privacy calls for an enterprise-wide proliferation of the privacy safeguarding principles, policies and practices, an organizational climate which insists on the development and consumption of enabling privacy enhancing technologies, and a culture that values privacy.

With the growing relevance of privacy, in this era of General Data Protection Regulation coming out of Europe, SMB leaders may comprehend the implications of reducing privacy concerns through policies, business processes and technologies that are permitted into their ecosystem. PbD is an organizational-enhancing opportunity which may be embedded into a business model (Cavoukian & Chibba 2018), to produce a needed organizational solution for current pains of employees. Even though some claim that privacy is dead (BBC:2017; Mims, 2018), the care for those who value privacy should not be overlooked. The privacy decision could be based purely on values of the stakeholder (Bryson et al., 2017). Vegh (2018) found that to achieve privacy by design according to GDPR, the following steps should be taken:

1. Perform a Privacy Impact Assessment (PIA) before including technologies into the ecosystem and before processing data subjects' data
2. Keep records of all processing and flow activities
3. Always ensure all data is protected at rest and in transit
4. Limit data processing
5. Limit data collection
6. Limit data access

If SBM leaders/agents ascribe to Vegh's steps, they would demonstrate that they value employee privacy, not only along the dimension of personal information privacy, but even autonomy and environmental privacy.

Considerations of privacy may be reflected in the architecting of the ecosystem. SMB leaders may be proactive and embed privacy by design and default aspects from the start and through every layer and component of the Internet of things (IOT) system (Apare & Gujar, 2018). Vegh (2018) clearly stated that privacy is not security, and this distinction can lead to the engineering of legally fit for use technologies. Business leaders should be aware of the disturbing patterns and behaviors that may result in informational and mental harm to employees, because of IOT (Apare & Gujar, 2018). This realization should be a reasonable basis for developing a privacy management program that mitigates against or prevents these harms to employees.

Some view the GDPR requirement compliance as a threat to technological advancements such as IOT, biometrics, artificial intelligence, machine learning, and blockchain. Using a value-focused perspective, GDPR can be an opportunity by which organizations uphold the human rights of privacy proclaimed by the United Nations in 1948. Organizational leaders can embrace the new ways of thinking, behaviors, practices, and expectations to craft relevant, aligned solutions for the safeguarding of privacy, and in support of organizational development and sustainability. Some characteristics of these privacy preserving solutions would be data minimization, informed consent, a legal basis for data collection, security during collection, transmission, processing, storage, accessing and disposition, and privacy preserving technologies, physical systems, and network infrastructure. Some security practices would be pseudonymization through encryption and steganography and anonymization (Vegh, 2018). Privacy researchers have presented options that SMB leaders may use to develop a robust privacy management solution that safeguards employee privacy.

Employee Privacy and the Internet

The privacy paradox dilemma of employees needs unpacking. Privacy is in crisis due to the use of surveillance technologies, online shaming, and profuse sharing of information on social media (Katsabian, 2019). There is a gap between theoretical implications of a desire for, and the actual practicing of, privacy. The privacy paradox dilemma is indicative of people willingly sharing more and more information with others, while at the same time wanting to keep the information private. These perceived contradictory behaviors may suggest that the employee does not value privacy and support Westin’s 1996 finding that employees are not interested in privacy.

However, this perception may be thwarted by the desire of data subjects to release personal information, to specific audiences, at times or to prefer that it is not in their purview. Employers, society, and employees are constantly blurring the lines of privacy, resulting in the privacy paradox dilemma (Katsabian, 2019). Under the more prevalent flexible regime of privacy, an employees' right to privacy may be easily and unknowingly eroded.

The flexible approach to privacy in this digital and connected era, is useful, but inadequate, and may require business leaders not taking advantage of the ambiguities that presently form this current dynamic. As such, a more procedural, predictable, consistent approach to this phenomenon may be warranted (Katsabian 2019; Solove, 2004). Even though the right of privacy is vague and elusive, there is an established benchmark under Article 12 Human Rights (2018). SMB leaders could remember these concerns when implementing measures to safeguard employee privacy.

Employer-employee experiences should be designed with the various interpretations of privacy in mind, not in a flexible manner, but in a human-centered co-created reasonable expectation of privacy. Warren and Brandeis (1890) presented privacy as the right to be left alone. Westin (1968) presented privacy as the right to secrecy with the preservation of autonomy, considering an individual and societal/group dynamic, a private time for self-reflection, separate personas – public and private, protected communication exchanges and the right to decide what should be disclosed. Privacy has also been presented as a right to limit access to self, as in a state of privacy, and the right to live freely (Katsabian, 2019). Katsabian (2019) has suggested that business leaders may:

1. Mandate anonymous CVs before the interview stage to prevent the screening of candidates at this preliminary stage based on Googling or just have a policy which does support Googling at the preliminary stage.
2. Create incentives for developing workplace-specific privacy rules in cooperation with employee representatives
3. Mandate a cooling-off period of one month before dismissals that are based on employees' private behavior.

Business leaders may consider these notions of privacy and embed privacy at the beginning, throughout and at the end of the employer-employee experience.

Employee Privacy and the Internet of Things

The monitoring of data running through a complex IOT system can prove complicated, complex, and costly. The use of Bring Your Own Device (BYOD) may add another layer of complexity, since devices are now so interconnected. Better and more comprehensive solutions for transparency in IOT systems are still needed (Li & Palinasamy, 2018). According to Singh and Kumar (2020), SMB leaders should develop solutions that support trustworthiness and authenticity in communications, confidentiality, integrity, authorization, since these are critical factors for the security and privacy of valued information assets. Employee privacy solutions that allow for authenticity, transparency, co-creation, and information security considerations are needed during this hyperconnected time.

The balancing of privacy friendly business practices, with shared data ownership and organizational need for transparency should be top of mind, for the contemporary business leader/agent. Privacy valuing business leaders may place privacy friendly business policies, processes, technologies, and network infrastructure, as a strategic effort for cultural adoption and institutionalization, in support of employee privacy (Anciaux et al., 2019). Data ownership, therefore, becomes a challenge in the IoT context, and so the basis of returning personal data, to data subjects seems to be a daunting challenge (Vegh, 2018). This intricate web that is being wirelessly woven, may suggest that employers can monitor and evaluate employees, but there may be ways to reduce encroachment and deep surveillance, for this end.

The breaches and secret data collection from connected inert devices have catapulted privacy researchers into the arena of the Internet of Things. Business leaders/agents may consider approaches to their IOT tech stack that preserve the privacy of their employees through techniques such as Differential Privacy, blockchain, privacy enhancing technologies (Li & Palinasamy, 2018). An awareness of the risks of inert connected devices, business leaders/agents, would help support a robust employee privacy management program.

Regulators and scholars considered the implications of the Internet of Things (IoT) since the 1970's in the United States of America. The precursor to the Privacy Act of 1974 (which only pertains to Federal Government bodies), the Health, Education and Welfare (HEW) Fair Information Practices (FIP) of 1973, purported the following five privacy principles:

1. No secret systems of personal data.
2. Ability for individuals to find out what is in the record, and how it is used.

3. Ability for individuals to prevent secondary use.
4. Ability to correct or amend records.
5. Data must be secure from misuse. (Li & Palinasmy, 2018).

FIPs was used as the basis for many organizational and industry guardrails for personal information privacy management. Even though the principles for the governance of information privacy was developed and used in other parts of the world, in the United States of America, no federal law was passed for control and management of the private information, reflective of the private affairs of all citizens.

Digital dossiers leave breadcrumbs all over the digital ecosystem and they are monetized and become part of the capitalistic surveillance economy. Even though it is very possible to track employees, business leaders should be considerate in the use of these wireless and connected devices, since the perceived loss of privacy, may result in serendipitous outcomes related to reduced trust, employee affective commitment, innovation, and creativity (Arnaud & Chandon, 2013; Dobson & Herbert, 2021; Dragano & Lunua, 2020; Tarafdar et al., 2019). Privacy-by-architecture or privacy-by-policy (Li & Palinasamy, 2018) are two approaches from which business leaders may choose to preserve the privacy of employee data during this digitizing era. SMB leaders could make use of these strategies and an understanding of the risks associated with the perceived loss of privacy by employees.

Employee Privacy and Big Data

Big data and analytical technologies have made it very probable that business leaders can mine and extract information on personnel that may be outside the bounds of their need to know. Radio Frequency Identification (RFID) badges, computer monitoring tools and Global Positioning Systems (GPS) may present a threat to employees' privacy, wellness, and autonomy (Areheart, 2019; Hornberger, 2021). The application of intrusive surveillance methods, tools and approaches, and data mining techniques wreak havoc on employees (Huppertz et al., 2020; Jovanović & Božičić, 2018; McParland & Connolly, 2020). The ease of access and use of analytical tools could facilitate malevolent patterned behaviors that can undermine the wellness and productivity of employees.

Balancing business needs and employee privacy is a tenuous, but considerate activity. Due to the ease of access and the inexpensiveness of virtual technologies, automatic processing, and the analysis of big data for decision making on potential and actual employees, has become easier (Katsabian, 2019). To glean information on productivity or trustworthiness, business leaders should not overuse surveillance technologies, as there may be serendipitous outcomes, such as increased work-related stress, mental discomfort, absenteeism, and reduced productivity (Jovanović & Božičić, 2018). As such, business leaders/agents may reconcile their business needs with those of the privacy expectation of their employees.

Employee Privacy and Working From Home Design

Working from home is now a viable option. Telework is a subset of remote work and work from home. Telework is defined as Information Communications Telework /mobile (ICTM) and mobile work (Katsabian, 2020). A hybrid of both has emerged during the COVID 19 pandemic. Leaders of SMBs should be aware of the impinging of the private sphere that could occur under this new workspace condition. As such, Katsabian (2020) suggested that employees be given a voice in the balancing of the public-private dynamic, in support of employees' rights to privacy. SMB leaders could involve their employees in discussions to arrive at an acceptable medium that balances the productivity needs and the employee's privacy.

This new work design has some benefits for both the employer and the employee. Katsabian (2020) noted the Gallop 2020 report which stated that approximately 62% of the American workforce is now teleworking. The employer and employee may experience some benefits such as cost savings and enhanced work-to-life balance. The home-office has given rise to new considerations, and concerns. Working from home could result in the hyper use of intrusive surveillance through third party technologies, by employers. To mitigate this risk, SMB leaders could co-create and communicate productivity expectations.

Employee Privacy and Surveillance Technologies

Surveillance should be balanced between a bona fide business need and the employees right to privacy. Since 1968, Westin presented this view of surveillance technologies in the business sphere. Current privacy researchers have suggested that overpowering and overbearing use of surveillance technologies may result in mental discomfort, reduced productivity, and increased stress levels (Dragano & Lunua, 2020; Tarafdar et al., 2019). SMBs leaders should bear the wellness of their employees in mind when selecting the capabilities of surveillance technologies. To mitigate these side effects of pervasive surveillance, business leaders should only collect data that supports the bona fide business need. Performance metrics could be utilized instead of observation during tasks. The negative stress due to oversurveillance could be mitigated against by the considerate selection of technologies, by SMB leaders.

New market dynamics and structures are evolving under this new digitalized regime and require more astute governance models. The rise of surveillance capitalism (Zuboff, 2019) has also produced new structural dynamics that reshape markets and the factors of production. Under this regime, employees' personal data sets can be presented to a data market and exchanged for profit. This operation may be occurring under the guise of wellness wearables. According to Zuboff (2019) business leaders/agents should not fall prey to the economizing and monetization of such assets. SMB leaders/actors/agents should guard against nefarious use of such intelligence by third party providers by developing policies for partnering engagements that reflect the valuing of the personal data of their employees.

Employee Privacy and Security

Due to the separate laws for security and privacy it is justified to conclude that security is separate from privacy. Security measures should be augmented with privacy preserving measures such as, personal data collection minimization, role-based access, separation, and anonymization (Hoepman, 2018). The loss of private information is an expensive business casualty, and as such, business leaders should implement a multi-tiered security strategy focused on prevention, mitigation, and response (Cook, 2017). Business leaders/agents should use the information on breaches that illustrate cybersecurity and physical security vulnerabilities, as a rationale for the development of robust privacy preserving practices. However, many organizational leaders are yielding to the zero-trust security paradigm, without understanding the need for privacy preservation capabilities within that ecosystem.

Security minimizes breaches of privacy due to loss, destruction, intentionally stolen, or unauthorized access. According to the HIPPA ACT, security refers to the specific measures and efforts taken to protect privacy, and to ensure the integrity of personal information (Pierre-Francois & Guzman, 2020). As such, security needs to be concerned with two information sets; personal information security and non-personal information security, where personal information is defined as information which can identify an individual (Keshu & Meixia, 2020). Cybersecurity could be blended with robust privacy safeguarding capabilities to reduce harms.

Complexity Leadership and Workplace Privacy

Safeguarding employee privacy needs to be balanced with economic, ethical, and security concerns of the business owners. Covert monitoring and the pervasive use of surveillance technologies could have negative outcomes on employee communication, creativity, stifle autonomy and authenticity (Arnaud & Chandon, 2013; Dobson & Herbert, 2021; Tarafdar et al., 2019). As a result, management decisions and ethical culture inside an organization will strongly determine how surveillance capabilities are leveraged toward competing goals. Uncontrolled monitoring creates an informational asymmetry, which when coupled with the over exposure and the aggregated information about the employees, results in inhibitions that could negatively affect business performance.

The use of artificial intelligence, biometrics, machine learning, and blockchain capabilities, should be tempered with knowledge of their limitations and issues, to support the rights of data subjects/rights owners. These rights have been defined in the General Data Protection Regulation (2018), for example - the right to be forgotten or erased. Westin's (1968) core privacy governance principle – control by fully knowledgeable data subjects – has been usurped (Zuboff, 2019). Yet, SMB leaders, as data processors can be mindful of using blockchain capabilities to securely transmit and store sensitive and personal information sets (Nortey et al., 2019). There are limitations regarding the right of erasure, by the data subject within legal allowances, that still need to be addressed.

Previous forms of monitoring have been overtaken by artificial intelligence, biometrics, machine learning, and blockchain capabilities. As such, the data collected should be securely stored, with authorized access and clearly delineated items for use (Adams et al., 2019; Jervis, 2018). The FTC (2018) also focused on the security plan aspect of privacy safeguarding. The FTC suggested five steps for developing a robust security plan – take stock, scale down, lock it, pitch it, and plan. The FTC also recommended that practitioners, take note of laws such as: the Gramm-Leach-Bliley Act (1999), the Fair Credit reporting Act (1970), and the FTC Act (1914). These are some frameworks for leaders of SMBs to look for guidance on the responsibility and accountability for personal and sensitive information.

Business leaders could be cognizant of the abuses that can occur during communication exchanges between the employees and their employers and implement processes that support personal privacy across the enterprise. Data and information management, along with the techno-ethics of personal privacy preservation, should be in the strategic and operational areas of the organization (Cortini & Fantinelli, 2018) for developing privacy programs that address these considerations. By incorporating these considerations into the privacy management program design and implementation, business leaders/agents may reduce the risk of harms to employees.

The decision to incorporate specific privacy processes to augment cyber technology has surfaced, since cybersecurity alone is not preventing privacy leakages or incidents. Few businesses are taking the necessary steps to safeguard their private data and enhance cyber security (Cook, 2017). Personal data such as a personally identifiable information (PII), sensitive information (SI) and personal health information (PHI) require careful handling to reduce the collection, minimize the storage, transmissions, and the access of such data sets (Kirk, 2018). Cybersecurity alone, does not prevent the leakage of private data, a harmonious approach of what is collected along with how the data is secured is a more robust solution.

From the roots of the FIPS ACT (1973), new relevant regulations have emerged to counter the power imbalances between data subjects and data processors. The General Data Protection Regulation (GDPR, European Union, 2018) has given rise to regulations worldwide that reflect the valuing of personal data. Under GDPR, “personal data” is broadly defined to include a person’s name, address, phone, email, as well as economic, social, cultural genetic, and mental characteristics. Photos, bank details, posts on social networking websites, political opinions, health information, computer IP addresses and more—are also considered personal data (Kirk, 2018). According to Uhl-Bien, (2021), the mandate for current organizational survival requires participants/actors, who are aware, adaptive, persistent, and confident under the pressures of complexity. Therefore, business leaders could assess their privacy and data security risks and implement policies and procedures that proactively protect employee privacy.

Complexity leaders could be aware of the many notions of privacy dimensions and the harms that may ensue due to poor or insufficient design considerations. Employee /Workplace privacy practitioners may focus on the informational, environmental and autonomy dimensions, and may co-create and communicate solutions that balance the need for employer productivity with the need for employee privacy. SMB leaders/agents could be mindful of the high complexity and scope of workplace privacy (Teebken, 2021). Technologies have progressed to enable the collection of granular observations of people, the combining of information, and the development of inferences, resulting in decisions and actions on a scale and at speeds not possible before (Zuboff, 2019). The balancing of the needs of the organization against the three areas of employee/workplace privacy may be a complex undertaking, mitigating the harms that can come from the ubiquitous gathering and processing capabilities of private information, is noteworthy.

This convergence of data monetization, granular observations, digital dossiers, and mental models of surveillance capitalism, along with the crisis of a pandemic, and resulting changes in remote work design have elevated the expectations from the employer-employee exchange. Leaders could simultaneously address risks to innovation, trust, employee commitment, employee wellness, organizational reputation, and productivity.

Transition

Section 1 was an introduction, which described the background of the doctoral study of privacy preservation phenomena, and strategies SMB owners employed to preserve employee privacy. Section 1 encompassed 12 major elements, which provided the overall foundation and scope of the doctoral study. Critical areas within the section included a background of the problem; the problem statement; the purpose statement; nature of the study; research questions; conceptual framework; operational terms; assumptions; limitations; delimitations; the significance of study; and summarization of professional and scholarly works of literature.

Section 2 restates the purpose statement; provides new subsections expanding on the roles of the researcher and participants, the research method and design, population and sampling criteria, ethical research criteria, data collection instrument and techniques, data organization and analysis methodologies, reliability and validity criteria mechanisms, and transitions into Section 3. Section 3 also provides the results of data analysis, findings, recommendations, and conclusions.

Section 2: The Project

The population for this multiple case study was three privacy practitioners supporting SMBs operating in the Mid-Atlantic region of the United States. The participants successfully safeguarded employee privacy and participated in semistructured virtual interviews. This section is organized into subsections and includes a presentation of the purpose of the research. A discussion of the research methods and design shows the rationale for inclusion. I discuss the sampling techniques, describe the population for the study, outline the ethical principles that guided the research, and discuss the principles for assuring the reliability and validity of the study.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the effective strategies that SMB leaders use to safeguard employee privacy. The multiple case study design is rooted in various people's conceptualizations and ideas (Saunders et al., 2018). As such, the targeted population for this study consisted of three privacy practitioner-consultants and SMB C-suite leader/agents from different firms located in the Mid-Atlantic region of the United States who successfully safeguarded employee privacy within their organizations. Additionally, purposeful participant selection criteria required that the selected SMBs (a) have a business address in the Mid-Atlantic region of the United States, (b) employ between one and 249 personnel, and (c) use privacy-safeguarding practices. The study could potentially effect social change by encouraging trusting employer–employee relationships that promote employee well-being and reduce turnover, which would be beneficial for both families and communities. This valuing of employee privacy by SMB leaders could improve business performance and thereby support the socioeconomic development of local communities.

Role of the Researcher

Qualitative researchers have many roles in the lifecycle of a research effort. According to Cook (2017), qualitative researchers are effective data collectors who subscribe to ethical standards and must analyze and interpret the collected data from a representative sample. The qualitative researcher must comply with ethical standards that ultimately result in doing the participants no harm. Researchers should comply with the protocols given by the Institutional Review Board (IRB) and the U.S. Department of Health and Human Services (DHHS) Belmont Report and protect participants from harm by keeping them anonymous, treating these individuals as autonomous agents, obtaining the research participation consent form, and providing participants with necessary protections (Cook, 2017). Simon (2011) also mentioned Greenbank's (2003) contribution that it is necessary to make potential consumers of research aware of a researcher's bias, assumptions, expectations, limitations, involvement, and experiences that qualified them to carry out the research. Whether a researcher has adopted an emic (insider) or etic (outsider) perspective should also be expressly stated (Punch, 1998). Researchers should clearly articulate the purpose of their study and their role in the research effort.

Integrity is expected from a researcher, and it is demonstrated through truthful reporting and display of findings. Researchers should truthfully report on findings and display the various perspectives that emerge from the collected data (Cook 2017). Guarding against researcher bias is also a consideration for developing a robust and reliable research study. To mitigate this bias, a researcher should use techniques such as triangulated data collection, seek data saturation, and perform member checking (Edwards-Brown, 2020; Yin, 2018). I used the triangulation of collected data from primary and secondary sources, noted data saturation, and performed member checking on my three participants to reduce researcher bias and to report truthfully on my findings.

A researcher's role is dependent on the method selected for the study and the collection method. According to Simon (2011), the role of the researcher varies depending on the type of method (i.e., quantitative, mixed method, or qualitative) and even within methods pertaining to the collection technique (e.g., narrative, focus group, or semistructured interviews). I used a semistructured interview for the data collection technique and a review of public-facing privacy document data. As a data collection instrument (Denzin & Lincoln, 2003), I was mindful of the pitfalls of these techniques and mitigated against the risks of researcher bias, as I mediated interpretation of the data being collected and analyzed. The interview protocol (Appendix C), member checking, and quick transcription afforded me ways to address this risk.

Techniques such as bracketing, reflexive journaling, and epoche support the validity of a research effort. Simon (2011) also discussed the use of a researcher journal that holds the researcher's personal reflections of self, past and present, and bracketing. According to Ahern (1999), bracketing is a means of demonstrating the validity of the data collection and analysis process (evolving findings). The researcher's ability to suspend judgement is of paramount importance to the validity of this effort. The researcher practices a recursive approach to data gathering (Simon, 2011). I used bracketing, reflexive journaling, and epoche to support the validity of my research effort.

Researchers should be able to put aside their knowledge sets, values, and preconceived notions and go in *tabula raza*, letting the experience generate the story. Researchers need to be mindful of how they carry themselves during the interview, reduce facial expressions to a blank slate, and use a neutral tone during the data collection process. According to Cook (2017), researchers should be (a) conscious and neutral in facial expressions, body language, tone, and dress, to not introduce bias with respondents; (b) ask questions without leading respondents; (c) refrain from offering an opinion; (d) strive for objectivity by recognizing their personal biases; and (e) report the collected data without prejudice.

I am a practicing organizational consultant working in the government contracting sector and familiar with the Mid-Atlantic area of the United States. I was familiar with the companies in this study. I was the primary researcher and data collection instrument for purposive sampling activity. In this multiple case study, I explored employee privacy safeguarding strategies that were being used by SMB leaders/agents. To be compliant with qualitative research protocols, I followed guidance articulated by Cook (2017) and clearly delineated the problem, background, rationale, objectives, research design and methodology, data analysis, and organization of the study. In accordance with Edwards-Brown (2020), I explained the process to the participants, monitored the process, extracted information from the various data collection sources, and provided valid and useful information for future researchers and business leaders.

Participants

There has been wide debate among researchers regarding the selection criteria and number of participants for a qualitative research study in the field of organizational and workplace studies that are necessary to establish credibility and utility with limited time and resources. According to Saunders and Townsend (2016), the credibility and utility of participant selection, number, and justification relate to the purpose of the study, study method and design, maturity of the phenomena, resources of the researcher, and researcher's guiding philosophy. For this study, in accordance with Saunders and Townsend (2016), I used a neo-positivist lens to justify my participant selection. I identified the number and characteristics of participants interviewed and reasons for their selection. Each participant had one interview, with questions that were specific to their role and responsibilities. I balanced representativeness with the quality of data by recruiting participants with various perspectives on the safeguarding of employee privacy phenomenon within a given time frame and resources.

For my study, I engaged three privacy practitioner participants: two C-suite leader/agents from small businesses in the Mid-Atlantic United States area and one consultant, all of whom demonstrated that they had successfully implemented the safeguarding of employee privacy. Although Cronin (2014) and Byers et al. (2014) suggested that four to 15 participants are desirable, the predominant focus is the collection of rich and thick data. To support the collection of rich, thick data, I used the multiple case study design. The functional selection criteria that I used for the business leaders/agents required them to be in the governance team of their organizations (i.e., C-suite), and since they were responsible for data governance, and/or privacy/security management that they would be knowledgeable in responding to the employee safeguarding practices and policies of their respective organizations. For the consultant, I used certifications in privacy management as an indicator that they would have knowledge on effective strategies for safeguarding employee privacy. The participants validated their qualifications during the interviews.

To ensure that I obtained rich data, I used participants who were qualified. I verified that the C-suite members operated their businesses from the Mid-Atlantic region through a Google address check. I noted the various privacy industry certifications for the consultant participant. I used the participants' responses to the details of the flyer as an indicator that the C-suite participants were experienced in effectively safeguarding employee privacy, through them having developed and implemented efficacious human resources management or practicing data governance by having information, privacy policies, or practices in effect. After receiving approval from Walden University and the IRB, I recruited qualified volunteers through my professional network and public channels such as Linkedin, International Association of Privacy Practitioners (IAPP), and Project Management Institute (PMI) forums.

To recruit qualified participants, I published the participant criteria in various channels and assumed truthful responses about participants' strategies for safeguarding employee privacy and trusted relationships. According to Cook (2017), to recruit participants, a researcher must consider building relationships with power players and influencers or leverage trusting relationships. I therefore published to various networks and leveraged trusted relationships to attract qualified privacy practitioners (SMB leaders/agents and consultants) to volunteer to participate in the study by highlighting the purpose and the benefits of the study for their organizational development. I presented the volunteers with the participant letter and consent form via email days before the actual interview. I contacted them to set the appointment for the recorded interview after they submitted "I consent" via email. I sent thank you emails after the interview sessions.

Cook (2017) listed prefieldwork actions that researchers use to develop rapport with study participants:

1. Conduct research on small- and medium-sized organizations.
2. Establish a mutual feeling of friendliness and highlight common interests.
3. Describe the research topic, the researcher's interest in the study, answer questions, and put participants at ease.
4. Reassure participants of data integrity throughout the process.
5. Reemphasize confidentiality.
6. Interact in a positive, professional manner; exhibit politeness and good manners.
7. Maintain a nonjudgmental attitude to ensure positive working relationships.
8. Show attentiveness by actively listening and engaging with participants throughout the interview activity.

After fieldwork, a researcher has other tasks to complete a study. Cook (2017) also suggested some postfieldwork actions. For instance, if insufficient data were collected or clarifications were needed, I would contact participants for clarification or follow-up discussions. Member checking was done to confirm interpretations of the interviews. I submitted data for member checking to participants via email, with a 72-hour response time. For those participants who did not respond in this timeframe to state issues or interpretations differing from the interpretation of the data, implied consent was deemed as accepted.

I ensured that my participants met the qualifying criteria for the study by using purposive sampling. According to Stake (2013), purposive sampling ensures that potential participants meet the eligibility criteria to take part in the study. To do this, I checked that the company address was for an office location in the Mid-Atlantic U.S. area. Through the broadcasting of the study, in both my professional network and a flyer, placed in various channels, I attracted qualified participants with the needed participant criteria for the study, who had been successfully implementing employee privacy safeguarding practices. Edwards-Brown (2020) noted that researchers build rapport with participants by explaining the purpose of their studies. As such, after I obtained expressions of interest from potential participants, and after I verified their eligibility, I sent each specific group of volunteers a formal invitation packet by email that included a participant letter and informed consent form, which explained the purpose of the study and instructions on how they could convey consent. Additionally, the consent form contained information on the data collection technique (i.e., synchronous recorded virtual interviews), the member checking process and expectations, and the process for participants removing themselves from the study. The informed consent form detailed the disposal plan for the recorded and confidential information by paper and electronic shredding and highlighted the following:

- purpose of the research
- participant's responsibility
- participant's right to answer some, all, or none of the questions without consequence
- my responsibility to keep all information and identifying characteristics confidential throughout the research process
- data retention plan for 5 years after publication of study
- disposal plan for collected data and personal identifiers (Edwards-Brown, 2020)

I sent one reminder email to potential participants and allowed them 72 hours to respond. After receipt of the signed consent forms, an interview meeting time of a half hour was set up that was convenient for both parties. The invitation to participate included the statement that any information shared during the interview would be recorded and would remain confidential and then be destroyed, as indicated above. By indicating "I consent" on the informed consent form or emailing the statement "I consent," the participants agreed to the requirements of the research process.

Research Method and Design

Research Method

When planning business research, researchers have a choice of three basic research methods: qualitative, quantitative, and mixed methods. I read several studies that used various methods while determining which method I would use in my study. I selected the qualitative method for my study because of the lack of empirical studies on the safeguarding of employee privacy in the U.S. private sector. According to Matt et al. (2017), using the qualitative method enables researchers to develop descriptions to understand dynamic processes. Researchers use the qualitative method to explore contemporary, real-life situations; capture descriptions of shared human experiences; and make sense and meaning of phenomena (Cook, 2017; Saunders et al., 2019; Yin, 2018). Alternatively, the quantitative method is appropriate when researchers use research measurement to test hypotheses for analyzing relationships among variables, and to make predictions and generalizations (Edwards-Brown, 2020; Saunders et al., 2019; Yin, 2018). Therefore, the quantitative method was not suitable for my study because the purpose of my study was to describe the employee privacy-safeguarding strategies that SMBs develop and implement, and not to develop theories or examine related variables. Using the mixed-method approach requires both quantitative and qualitative research techniques to address complicated research questions, develop a deeper theoretical understanding, and elaborate upon findings of qualitative data (Pervez et al., 2021; Saunders et al., 2019; Yin, 2018). As such, the mixed method was not appropriate for my study because I did not need the quantitative method to identify and explore the effective strategies that SMB leaders use to safeguard employee privacy.

Research Design

I selected a qualitative multiple case study design for my study to derive differences and similarities of the privacy safeguarding phenomena. I also considered the appropriateness of the ethnographic and phenomenological designs. Through a qualitative multiple case study design, a researcher can explore *what, how,* and *why* and obtain details and perspectives concerning a specific situation replicated across more than a single case (Creswell & Poth, 2016; Gustafsson, 2017; Yin, 2018). The multiple case study research design also rapidly captures the rich perspectives of the various human capital management strategies employed at various levels of an organization and facilitates understanding of the patterns of findings from interviews and questionnaires developed across cases (Yin, 2018). In contrast, a single case study, as posited by Gustafsson (2017) would not have provided me with depth and breadth of information on this employee privacy-focused phenomenon. The multiple case study design provided me the opportunity to gather rich information from various viewpoints for possible comparisons across cases.

Use of the ethnographic design requires a researcher to be immersed in the cultural practices of a group (Cook, 2017; Miller & Slater, 2020; Zilber, 2020). The ethnographic design was not a fit for my study, because I did not immerse myself in the organizational context, as a participant observer, or employ the safeguarding strategies for employees in the selected SMBs. Through the phenomenological design researchers explore the meanings of the lived experiences of an individual or group of people related to a unique phenomenon (Cook, 2017; Mayoh & Onwuegbuzie, 2015; van Manen & van Manen, 2021). The phenomenological design was not appropriate because I did not need to explore the personal meanings of participants’ lived experiences during this study.

Population and Sampling

For my multiple case study, the population comprised privacy practitioners who were successfully safeguarding employee privacy, as indicated by their having human resources management, or data governance – information, privacy policies, or practices (formal or informal) in effect, or the achievement of pre-established employee privacy initiatives or having been successful in completing consulting assignments. For my study, I used purposeful sampling. Purposeful sampling is a common process used in qualitative research, by which a researcher may collect pertinent data due to the identification of people, who meet the qualification criteria to participate in the research study for a better match to the aims and objectives of the study (Campbell et al., 2020; Etikan et al., 2016; Ngozwana, 2018; Yin, 2018). I qualified my participants by informing them on the purpose of the study and noting that they supported SMBs with the safeguarding of employee privacy. I collected pertinent data through two sources - semistructured interviews and public facing policies and blog. The sample matched the aim and objective of my research study which was to explore the safeguarding strategies for employee privacy used by privacy practitioners who support small-midsized businesses situated in the Mid-Atlantic region.

The researcher should verify that data saturation is reached. Data saturation is noted when no new data, no new themes, no new coding emerge, and there is an ability to replicate the study (Fusch et al., 2017). I verified data saturation was reached within the selected sampling size of three interviews, when through thematic analysis, involving rounds of coding and interpretive activities, no new information was generated.

The researcher should mitigate the use of personal lens bias. According to Ahern, (1999) and Shufutinsky (2020), the researcher minimizes the risk of personal bias during the data collection, interpretation, and presentation events of the study by using bracketing and epoch tactics. As the principal instrument of analysis, I practiced bracketing, by identifying my biases from my previous experiences in privacy management and mitigated interference in the research process. I practiced epoch, which is the conscious suspension of my beliefs, values, judgements, and knowledge during the various events of the research process.

Ethical Research

Assuring research was conducted in an ethical manner requires a concerted determination from all parties involved to facilitate truthful, complete responses and ample controls for security and confidentiality of collected data, for demonstrating trustworthiness and for ensuring confidence in the overall process and products of the study. Ethics relates to doing good and avoiding harm (Childress & Beauchamp, 2022). One means for assuring ethical research is that of requiring a research ethics board review, which provides protocols and policies for how the research can be conducted and, on the behavior, and expectations of the researcher (Cook, 2017). Ethical research is best carried out by researchers who have taken the needed ethics training and commit to practice the procedures and protocols presented therein. For my study, I followed the recommendations for research ethics and standards provided by the National Institutes of Health (NIH) and satisfactorily completed the required training course on protecting human research participants and obtained Walden University's IRB approval, before executing the study.

A qualitative study requires that the researcher be mindful of boundaries between themselves and their participants. This requirement necessitates the researcher, as a data collection instrument, mitigates against concerns that may arise before, during and after, the study has been executed (Aluwihare-Samaranayake, 2012). As such, to provide adequate evidence of care, and to support confidence for the ethical design and execution of the study, the researcher should be guided by principles of the U.S. DHHS for human subject research. These protocols and guidelines, and the Belmont Report (DHHS, 1979) mandate adherence to respect, beneficence, nonmaleficence, and justice (Aluwihare-Samaranayake, 2012; Cook, 2017). During my study, I stayed aware of the boundaries between myself and my participants, I supported my participants' autonomy by obtaining their informed consent and practicing confidentiality. I also followed the IRB protocols to reduce possible harm, and I will share a summary of my study's findings with all three participants.

As the principal data collection instrument, the qualitative researcher plays an integral role in defining the quality and integrity of the research effort. Through ethical reflexivity, the researcher examines their thinking, biases and context, relevance, and impact of the study. To this end, the researcher must use fair procedures for selection, treatment and equitable distribution of benefits and burdens to all participants as governed by the DHHS principles (Cook, 2017). For assuring ethical studies, the researcher should consider the following issues: (a) informed consent, (b) confidentiality,

(c) data security, and (d) the voluntary nature of participation (Simpson, 2018). Demonstrating achievement of these characteristics would support the trustworthiness of the study and the resulting findings.

I adhered to the ethical principles and guidelines for the protection of human subjects as described in the Belmont Report while conducting this multiple case study research. To demonstrate the trustworthiness factor, I followed Cook's (2017) guidance and: (a) adhered to ethical research practices, (b) focused on the context of the study, (c) participated only as an outsider, (d) adhered to the interview protocol, (e) protected the privacy of participants, (f) maintained the confidentiality of the data, (g) guided the conversation and refrained from leading questions, (h) avoided reactions based on respondents' responses, (i) objectively interpreted the data obtained from participants, (j) utilized member checking, and (k) maintained an audit trail during the research process. I also ensured that the final doctoral manuscript included the Walden IRB approval number 02-23-22-0343418 and listed all agreement documents in the Table of Contents and appendices.

Informed Consent

Informed consent is an ethical expectation, and during my study, I established and complied with a documented procedure that protects the rights of participants and upholds the ethical value of participant autonomy and competency to agree (Cook, 2017; Roth & von Unger, 2018). Informed consent is a needed precursor to collecting data from human participants. For my study, I obtained participants' agreements to participate in the study, only after the participants were informed on the potential benefits and risks to themselves and society at large, the security and confidentiality protocols that were put in place for their protection. The study, participants completed and returned the consent forms, or provided documentation of consent, prior to the interviews and document collection.

Confidentiality

For my study, I ensured confidentiality, by restricting access to specific data sets, I obfuscated the identification of study participants and to demonstrate compliance with research standards, I obtained the IRB number 02-23-22-0343418, as evidence that the proposed study passed an ethics board review. In support of confidentiality, personally identifiable data of participants was obfuscated during the data collection and analysis phase (Cook 2017; Roth & von Unger, 2018; Quieros et al., 2017). As such, for confidentiality, during the data collection phase, I assigned pseudonyms to the three participants that were also used during the analysis phase. I assigned the following codes to the participating SMB leader/agents: PC1, P1Cs, P2Cs. The IRBs ensure that there are adequate provisions to protect the privacy of subjects, and to maintain the confidentiality of data, prior to approving a study. As such, before I began the study, I followed the guidance given by Walden's IRB and my committee's oversight to verify compliance with the approved IRB application.

Participation was voluntary, and I verbally and in writing, informed participants that they could have withdrawn at any time, by giving me notice via email, or phone. For my study, participants demonstrated their consent to participate when they returned an email which stated, "I consent". In accordance with established guidelines, I will securely retain the data and documents collected for a period of 5 years after the publication of the study. After the 5 years, I will electronically and manually shred all files associated with the study.

Data Collection Instruments

I was the principal data collecting instrument for the proposed qualitative multiple case study. I collected data according to following Yin's (2018) four principles: 1) use of multiple sources of evidence, 2) create a case study database, 3) maintain a chain of evidence to increase reliability of the information, and 4) exercise care when using data from electronic sources. Yin (2018) suggested using at least two of the six sources for collecting data for case studies: 1) interviews, 2) archival records, 3) documents, 4) direct observation, 5) participant observations, and 6) physical artifacts. I kept recruitment and data collection logs per Walden University's standards.

In my study, the data collection sources included semi-structured, virtual interviews and review of privacy documents. I created a detailed audit trail to maintain an organized collection of materials involved in the study. As suggested by Castillo-Montoya, (2016) and Kallio et. al. (2016), I used the interview refinement protocol to develop the interview protocol in (Appendix C) to establish a trustworthy, objective, and reliable data collection process. I held semistructured recorded interviews, via the web, to collect data from participants selected for the study. This technique was viable and feasible during this post pandemic period to assure the safety of both the researcher and study participants. I reviewed web-based public facing privacy documents and blogs that described or illustrated the employee privacy safeguarding strategies.

To achieve methodological triangulation, I collected data using the virtual synchronous interviews from consultants and C-suite leaders, and a review of privacy documents. For the interviews, I developed specific open-ended questions for each of the 2-privacy practitioner group: consultants and C-suite leaders. I obtained IRB approval for the interview protocol and interview questions (Appendix C), before I contacted participants or executed the interviews. Before starting the interviews, as suggested by (Edward-Brown, 2020), I reviewed the interview protocol, to assure that there was sufficient time to conduct the interviews with minimum inconvenience to the privacy practitioners – consultants, and SMB leaders/agents. During the data collection efforts, for the interviews, I created an atmosphere for the participants to be at ease when sharing their experiences by ensuring that they were informed on the expected duration for the interview, and that they had the interview questions before hand.

Data Collection Technique

For my study, the data collection sources were determined by the research purpose and question, and considerations for the proposed participants (where they can be reached, equitable distribution of benefit/burden exchange, required infrastructure, sensitivity of topic and respondents' feelings). During the data collection activity, I collected data from both primary and secondary data sources. For primary collections, I used semistructured recorded, virtual interviews, and for secondary sources, I reviewed public facing privacy documents - blog and employee privacy policy. An advantage of personal interviews in qualitative data collection is that they capture human interactions, emotions, and allows for the researcher to ask follow-up questions to unearth deeper, richer understanding of phenomena (Marshall & Rossman, 2016; Pacho, 2015; Yin, 2018). A disadvantage of interviews may be that interviews are more time and cost consuming, since it involves transcription, organization and reporting, and alternative use of time by participants. Another disadvantage is the dependency of the quality of the data collected on the researcher interview capabilities, and as such, the researcher needs to manage bias, and reactions.

For the primary data collection source - the synchronous semistructured virtual interviews, I used a synchronous virtual platform, as an alternative to in-person face-to-face interviews. Researchers have stated that technological advancements such as Voice over Internet Protocol (VOIP) tools as Skype and FaceTIme, and infrastructure have made it feasible for researchers to use these modes of communication to reach dispersed research populations using synchronous connections with confidence (Deakin & Wakefield, 2014; Janghorban et. al., 2014; Lo Lacono et. al., 2016). This approach was viable in the COVID 19 pandemic period for the study.

The interview protocol was critical to the quality of data collected from the interviews. I, therefore, developed an interview protocol that provided guidance on the pacing, sequencing, and facilitated a consistent repeatable process for completing effective and efficient interviews. For the synchronous virtual interviews, I developed open-ended interview questions on strategies for safeguarding employee privacy. Before the actual day of the interview, I sent out a consent process and research purpose and information document, to the qualified, self-reporting participants This communication informed the participants on how they could have withdrawn their agreement to participate and share information at any time, and that their information would be confidential. I also shared the nature and purpose of the study with the participants and reminded them that they were free to terminate the interview at any time, as stipulated in the consent form.

I used audio recorded interviews and conveyed the purpose of such to the consenting participants. Participants should be informed on the purpose of the recording, as assurance of an accurate transcription of their participants' responses (Crozier & Cassell, 2016). Member checking is an activity which enhances data quality, reliability, and trustworthiness (Yin, 2018). The process provides an opportunity to review interpretations of the responses for resonance with participants, and to summarize the replies to the interview questions (Edwards-Brown, 2020). I used the transcription to interpret their responses and presented those interpretations via the member checking activity, to the participants for confirmation or modifications.

I used public facing privacy documents as a secondary data source. I reviewed the public facing privacy documents that described or illustrated the employee privacy safeguarding strategies that some organizational leaders/agents have developed and implemented. An advantage of reviewing public facing documents as a data source, is that it is immediate, and easily accessible. However, a potential disadvantage of reviewing public facing documents is that they may not suggest the intent of the organizational direction nor align with organizational practices, and it may be difficult to ensure validity and reliability.

Data Organization Technique

The overarching goal when considering data organization techniques is ensuring ethical research practices including protection of privacy and confidentiality of participants (Saunders et al., 2016; Yin, 2018). To achieve sound data organization, I logged all recruitment and data collection processes and contact events. I also stored all data, including (a) written and electronic notes, (b) digital voice recordings, and (c) e-mail messages in a secure manner in accordance with IRB guidelines (Walden University, 2019). Secure storage of data was assured by using password protected electronic files stored in a secured cloud-based storage requiring limited authorized access. I will also, retain the secured hard and electronic files for five years from the completed publication of the study, and then destroy the electronic ones through a virtual shredding service.

Data Analysis

During the data analysis phase, I used both the manual and computer aided methods to conduct a thematic analysis of the collected data. I also used the NVivo version 12 qualitative data analysis (QDA) computer software package. Using this package helped me to organize, analyze, visualize, and find insights in unstructured or qualitative data like the interviews and privacy documents. The data analysis process is recursive in nature (Castleberry & Nolen, 2018). I used a combined technique of inductive and deductive thematic analysis. I used an a priori list developed during literature reviews on the topic and blended conceptual framework- CT and CL (deductive) and inductive analysis from compiled sources, for the emerging meaning from collected sources – i.e., interviews and privacy documents. According to Castleberry and Nolen (2018), and Saunders et al. (2015), thematic analysis allows the researcher to explore and analyze common threads and recurring themes within the conceptual framework, interviews, observations, documents, and data sets from literature reviews (including new studies published since writing the proposal). Thematic analysis is a form of pattern recognition within the data, where emerging themes become the categories for analysis (Castleberry & Nolen, 2018).

To summarize collected data a researcher may use thematic analysis. Thematic analysis transcends summarizing collected data such as study interviews for (a) interpreting, (b) understanding, and (c) explaining the underlying themes through deep critical thinking and analysis (Maguire & Delahunt, 2017). Thematic analysis proceeds by identifying and merging data with common threads for identifying key themes and developing explanations based on the interpretation of the data (Saunders et. al. 2015). During my study, it was important to demonstrate rigor in the analytical process. According to Castleberry and Nolen, 2018, Saunders et al., 2015, rigor in the analytical process, is to assure trustworthiness, credibility, and transferability and research quality. Using thematic analysis contributed to assuring my research findings are derived from complying with the highest academic standards.

I used Castleberry & Nolen's 2018, five-step process to analyze the collected data. The first phase of this data analysis process was the compilation phase. I gathered and organized all data – structured and unstructured data sets into a useable form for finding meaningful answers to my research question. According to Erlingsson and

Brysiewicz (2017), transcribed interviews text serves as a good starting point for content analysis in qualitative research. As such, I transcribed the virtually recorded interviews, using transcription software and adjusted them for analysis and familiarized myself with the contents of the transcripts, through rounds of readings and note-making. I collated responses and organized other textual data to be included in the analysis.

Once the data had been compiled, the second step of Castleberry & Nolen's five-step process was stratifying the data into common threads and patterns, which is defined as disassembling, in which the researcher could choose to adopt a coding strategy based on using prior research or theory (a priori), or use coding based on descriptions of patterns that emerge or In Vivo coding according to the verbatim words or phrases from the data sources in the research study (Castleberry & Nolen, 2018). While there is computer assisted software that can help to identify and group based on common themes, the researcher still has the responsibility to conduct the review and analysis (Castleberry & Nolen, 2018; Saunders et al., 2015).

I did a manual sorting of the contents according to common themes, based on my knowledge of the research question and intuition, that were then assigned a code to aid ease of retrieval, analysis, and interpretation. I developed codes using the combined deductive and inductive techniques of the emerging meaning from the interviews and review of the privacy documents, and the a priori list of themes compiled during literature reviews on the topic and the blended conceptual framework- CT and CL. A researcher may select a combination of coding methods for their study and may use a descriptive coding method to ascribe meaning to names, roles of categories derived from reasoning processes or the In vivo coding technique which uses the captured verbatim words or phrases to categorize the unit of data (Castleberry & Nolen, 2018). I used a descriptive - coding method. During the disassembling step, I manually identified similarities and differences in concepts, themes, and ideas, from the collected data, and literature review, and developed codes for each group and sorted them on an Excel spreadsheet. I then used the computer aided software – NVivo. I uploaded the sources of information into the program, created files, cases, and classifications and I ran auto coding on the Literature Review to produce a priori list of codes. NVivo cannot independently reduce, identify groups or categories, or seek understanding. I needed to perform further steps to obtain results from the organized data sets.

In reference to the third step – reassembling, Castleberry and Nolen (2018) emphasized that the researcher can adopt either a hierarchical or matrix model to identify and describe themes which when interpreted, help to answer the research question. These tools reduce qualitative data and highlights relationships among codes, cases – contexts and groups. For my study, I reassembled using a hierarchical model to convey how themes are subordinate or superordinate to each other. I then selected the mother and children codes that best answered my research question and ran various queries using code to cases to obtain emergent information from the data sets. I used word frequency queries and visualization tools to reveal patterns and develop interpretations.

During the interpreting fourth step, I made analytical conclusions from the data represented as codes and the themes generated from them. Yin, 2018 presented five qualities that should be the goal of all qualitative interpretations - 1) complete, 2) fair, 3) accurate, 4) representative of the data collected, add value to our understanding of the topic; and 5) be credible and gain respect from colleagues. According to Castleberry and Nolen (2018), interpreting should happen during the other steps, emerge easily from the data and form the foundation for the conclusions. I listed and revisited conclusions along the way. I developed a thematic map, such as word clouds and word trees, and clusters to visualize the relationships between codes and themes.

According to Castleberry and Nolen (2018), in the fifth step, the researcher forms responses to the research question or purpose of the study. My conclusions were based on the analyses of the developed codes to cases and emergent themes. To assure validity, I demonstrated how the previously developed codes and their patterns justified the themes and the resulting interpretations.

Reliability and Validity

Traditionally, reliability and validity are concepts used to evaluate the quality of research. Saunders et al., (2019) indicated that the credibility of research findings was viewed through the lens of two parameters on research design - reliability and validity. Trustworthiness of qualitative research was presented as a quality defining criteria (Lincoln & Guba, 1985). Some social researchers insist that qualitative researchers could develop and utilize their own evaluation criteria, so that the research is validated and deemed reliable, and to expand techniques, tactics in the field of qualitative research (Prakke & Wurster, 1999). For my study, I did not develop and utilize my own evaluation criteria. Instead, I used the trustworthiness criteria to reflect the quality of my research.

Reliability

Reliability (dependability) of a qualitative study entails the extent to which research findings are consistent (Yin, 2018). In quantitative research, reliability is the ability of a study to be repeated and result in similar findings (Leung, 2015). To support reliability, the qualitative researcher should address dependability. The researcher can ensure the dependability of the study through member checking, transcript review, expert validation of the interview questions, triangulation, using the interview protocol, and reaching data saturation (Yin, 2018). For my study, I ensured reliability (dependability) by sending each participant their interpretive file for their review; when no new information was added, data saturation was met. I also had experts review my interview questions, I used the interview protocol, practiced triangulation of sources – interview responses, from various perspectives and public facing documents.

Dependability

This criterion considers the due diligence and care that was taken from the problem identification, study design selection through to the execution of the study and the development of the findings. To establish this, I used member checking, which according to Smith and McGannon (2018), involves a process by which participants confirm or refute the trustworthiness or credibility of the findings of the qualitative data analysis. My member checking activity is dependable, due to the demonstrated due diligence and care that I took throughout this study.

I also used expert validation of the interview questions, triangulation - data source and method. I used the interview protocol. The interview protocol is a list of guidelines that navigates the researcher through each interview and provides a systematic and repeatable approach to ensure each interview is conducted in the same manner, thus mitigating bias during the interview process, and enhancing the authenticity of the process and interview data (Grossoehme, 2014; Edwards-Brown, 2020). The researcher can ensure the trustworthiness of the research, by asking appropriate interview questions and appropriately documenting the processes along with the logic behind the decisions reached during the research analysis process (Kyngäs et al., 2020). I ensured trustworthiness by asking expertly reviewed interview questions that were aligned with the research question, documenting my decision logic during my research process, and using the interview protocol for consistency and to mitigate bias.

Validity

To ensure these quality criteria were met and demonstrated in my study, I used tactics such as: member checking, triangulation, data saturation, and the use of an interview protocol. These tactics support the intention to provide trustworthy findings. Validity in qualitative research is analogous with credibility, transferability, and confirmability of findings (Cypress 2017). As such, as a social researcher, involved in a qualitative research project, I was intentional in presenting the four aspects of trustworthiness as defined by Cypress (2017) - credibility, transferability, confirmability, and dependability (discussed under reliability) of the study. To this end, I established:

Credibility

This criterion demonstrates that the findings of the study are rooted and reflect the actual experiences and perspectives of the participants - i.e., respondents, and interviewees. Liao and Hitchcock (2018) reported that there are two considerations to achieve credibility; (a) primary techniques which include design, sample, and data collection and (b) additional credibility techniques which include triangulation, audit trail, member checking, and persistent observation. To assure and demonstrate credibility, I used a systematic process to mitigate the risks of enquirer biases that may contaminate findings. To this end, I did member checking of the data interpretation - this is a technique in which the data, and interpretations, are shared with the participants. Member checking allowed participants to verify and clarify what their intentions were, correct errors, and provide additional information if necessary.

Transferability

This criterion demonstrates how I will enable others to determine the extent to which the study's findings may be applicable to their research domains. Transferability means enabling others to form conclusions, if findings from particular research apply in a different field or location (Liao & Hitchcock, 2018). To facilitate others' determination of transferability of my research, I provided an audit trail, to document all the steps taken in the research project, and an interview protocol to ensure thorough description the study's design and the design's implementation (Yin, 2018). For future researchers, I prepared interview summaries to be shared with comparable participants who were not enrolled in this study. If the researchers find similar trends or themes, and they choose to use the findings from this study, then I will have enabled others' determination of the study being transferable. For example, Liao and Hitchcock (2018) explained that to encourage others to determine the transferability of the findings of a study, researchers could provide rich descriptions of the context of the research and rich descriptions of the participants' accounts. I provided rich descriptions of the context of the research and the participants' accounts.

Confirmability

Addressing the confirmability criterion require me to ensure that the findings and conclusions I develop and communicate can be confirmed by others. Establishing rigor of qualitative research requires providing an unbiased and thorough representation of the participants' responses, through comprehensively documenting and describing the processes for collecting, analyzing, verifying the data throughout the study (Bearss et. al., 2016; Lincoln & Guba, 1985), and having the researcher engage in a deliberate reasoning process of inferring claims from their data beyond procedural templates (Harley & Cornelissen, 2022). I, therefore, documented and detailed a data audit trail of events such as the interview process and sample selection, data analysis techniques, identification of themes, researcher expectations, knowledge and participant relationship, IRB protocols, and noted in my journal my line of reasoning for arriving at the claims from the data.

I used triangulation of data sources (from various points/perspectives– Consultants and C-suite) and method triangulation (various data collection methods – interviews and web-based docs - privacy related docs and blog). The researcher could enhance rigor in qualitative research by means of triangulation (Marshall & Rossman, 2016). Triangulation decreases biases, increases validity, and strengthens the research, enhances rigor, and trustworthiness of the study, and produce more comprehensive findings (Edwards-Brown, 2020; Cypress, 2017; Smith & McGannon, 2018). My use of triangulation in my study decreased bias, increased validity, enhanced its rigor and trustworthiness, strengthened my research, and produced more robust findings.

Establishing researcher capabilities, experiences, knowledge, and biases are also part of the confirmability criteria. As such, I clearly stated my experiences, knowledge in the field of privacy and business consultancy, and defined my relationship to the research participants. I incentivized participants by offering a $20 e-Gift card for completing the study and offered to present them with copies of the research findings, in exchange for their agreement and volunteer participation. I established my researcher capabilities by practicing the behaviors identified in the IRB protocols, to cause no harm to my human participants. In accord with Lincoln and Guba (1985) and Saunders et. al., (2019), I sought to mitigate participant and researcher bias and error by documenting and detailing a data audit trail of events such as the interview process and sample selection, data analysis techniques, researcher expectations, knowledge and participant relationship, and IRB protocols. I interviewed three privacy practitioners – one consultant, and two C-suite business leaders of small and midsized companies located in the Mid-Atlantic region of the USA, with experience in successfully developing and managing employee privacy initiatives. Qualitative researchers boost credibility of research when the participants of a study review the information (Marshall & Rossman, 2016). I used an established interview protocol (Appendix C), during collection, and during data analysis. I invited participants to review the data interpretation through member checking via email and gave them 72 hours to review and submit any changes to the interpretive files. None of the participants added anything further or changed anything during this member checking activity.

Data Saturation

Data saturation is a technique that researchers use to support the robustness of a study. According to Saunders et al., (2017) data saturation should be used in a manner that is consistent with the research question, the theoretical position and analytic framework that is being adopted for the study. I intentionally, ensured that my themes aligned with my research question, and used a prior list from the literature review to assist with the coding that may have emerged from the thematic analysis of the collected data sources. When using the NVivo software, I adjusted the autocoding output since the outputs were too numerous. Data saturation is achieved when no new data, no new themes, no new coding emerge, and there is an ability to replicate the study (Fusch et al., 2017). During the manual analysis, I used a hierarchical matrix to place some descriptions under more noted headings of autonomy, environmental and personal information privacy. Through rounds of analysis, I documented, organized, and sorted, the various themes and subthemes from the multiple data sources, until no new relevant themes, emerged. Data saturation was demonstrated when I queried the data sets and no new coding themes emerged in relation to the research question.

Transition and Summary

Section 2 restated the purpose statement; provided new subsections expanding on the roles of the researcher and participants; the research method and design; population and sampling criteria; ethical research criteria; data collection instrument and techniques;

data organization and analysis methodologies; reliability and validity criteria mechanisms; and transitions into Section 3.

Section 3 includes an overview of the qualitative multiple case study, presentation of conclusions based on the collected research data and analyzed results, application of the study to professional business practices, and potential implications for social change. Additionally, I provide recommendations for modification of workplace privacy business practices for SMBs leaders/agents based on analysis through methodological triangulation of all my data sources such as: examination public facing privacy policy documents, blog, literature review and the semi-structured, digitally recorded interviews. Lastly, Section 3 contains recommendations for action, recommendations for further research, my reflections and experience within the process, and the DBA Doctoral Study's conclusion.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative multiple case study was to explore effective strategies that SMB leaders/agents use to safeguard employee privacy. The specific population consisted of three participants from two groups—consultant and C-suite leaders/agents from SMBs who had successfully implemented workplace privacy strategies. The composite conceptual framework for this study was CT and CLT. Public documentation, blogs, a priori codes from the literature review, and participant interview responses provided the data sources that I used to address the research question. Three major themes emerged: (a) an awareness of culture and value systems is necessary (environmental privacy), (b) surveillance capabilities are not currently being used by the C-suite leaders/agents (autonomy privacy), and (c) a predominant focus on the safeguarding of personal information assets using technological and InfoSec practices and policy controls (personal information privacy). My analysis of the research study findings suggests some effective strategies that successful SMB leaders/agents could use to safeguard employee privacy.

Presentation of the Findings

The central research question for the study was the following: What effective strategies do SMB leaders/agents use to safeguard workplace privacy? I used review of public documents, blogs, and semistructured recorded interviews with reviewed open-ended questions and the literature review as data sources for my study. I achieved data saturation when the interview respondent data, public documents, blogs, and a priori documents I reviewed became repetitive and no new information materialized.

As the primary research data collection instrument, I did both a manual analysis and a computer-aided technology analysis using NVivo (Version 12). Manually, I created a database in Excel and maintained an audit trail of study participant correspondence, journal notes, and documents. In NVivo, I organized, coded, analyzed, and visualized the study data by importing public documentation, participants' answers to the interview questions, the member-checked interpretative files (adjusted for analysis), and interview notes. Reviewing the public documents, which included a public-facing employee privacy policy and a blog, and the findings from participant interviews, enabled the process of triangulation for assuring conclusion validity and identifying common themes.

I conducted three semistructured interviews over a period of 4 weeks. The codes I used for participants in the study were for the one consultant (P1C) and the two C-suite leader/agents, P1Cs and P2Cs. CT and CLT provided the composite conceptual framework for exploring the overarching research question of this qualitative multiple case study. The findings corroborated those of Ball et al. (2013) that there is a predominant focus on the personal information privacy dimension, both in literature and in practice. Three major themes emerged from the triangulated data analysis: (a) an awareness of culture and value systems is necessary (environmental privacy), (b) surveillance capabilities are not currently being used by the C-suite leaders/agents (autonomy privacy), and (c) a predominant focus on the safeguarding of personal information assets using technological and InfoSec practices and policy controls (personal information privacy).

Table 2 reflects a summary of my findings across codes (rows) that emerged from the manual and NVivo analyses. The codes have been extracted from the various data sources (three interviews) and placed into the three workplace/employee privacy dimensions found in the literature. P1Cs and P2Cs refer to the C-suite participants, and P1C refers to the consultant participant. The member-checked interpretive transcripts were adjusted using computer-aided analysis to remove unnecessary words or expressions. The reviews of the secondary sources confirm a focus on the safeguarding of the personal information of employees by practitioners and considerations for autonomy and environmental privacy. The secondary sources augment the primary sources by introducing offensive and defensive safeguarding strategies. Some offensive strategies are related to data sharing, storage, collection, and deletion protocols, and some defensive strategies are related to the informing of employees on privacy-enhancing technologies.

Table 2

Categories and Presence of Codes for Successful Safeguarding of Employee Privacy

Codes	Interview P1Cs transcription—Adjusted for analysis	Interview P2Cs transcription—Adjusted for analysis	Interview P1C transcription —Adjusted for analysis	Manual analysis results	Workplace/ employee privacy dimensions
Monitoring	1	1	0	1	Autonomy
Surveillance	1	1	0	1	Autonomy
Culture	1	0	1	1	Environmental
Telework	1	1	0	1	Environmental
Authorized access	1	1	0	1	Personal information
Local storage	0	1	0	1	Personal information
Need to know	1	1	0	1	Personal information
Password protections	1	1	0	1	Personal information
Segregation	1	1	0	1	Personal information

Emergent Theme 1: Culture and Value Systems (Environmental Privacy)

The codes to cases (data sources) query and analysis revealed that for the participant pool and topic under research (employee privacy), there was a high level of control tactics being intuitively used by the small business agents/leaders. For instance, P1Cs stated that “I have modeled the safeguarding of privacy of employees, as personal information, in a way that I manage my own files. We have an official record system and then we have working files.” At another time, P1Cs stated, “I think I've leaned very heavily on the technology tools. I think the strategy of building the culture or awareness or training is needed.” P1C also stated, “It [privacy] is a very tricky area.”

Through the composite conceptual framework of CLT and CT, I expected to find that SMBs were complex adaptive systems that, through their leaders/agents' sensing and valuing, could self-organize, self-produce, and self-correct, in accordance with the literature presented by researchers such as Baltaci and Balci (2017), Liechtenstein (2008), and Uhl-Bien (2021), and that the concept of employee privacy would be viewed as complex, as posited by Katsabian (2020) and Solove (2004). The findings corroborated these expectations when P1Cs recognized that there were current gaps in the approach to employee privacy that needed to be filled, and that adjustments would have to made to the organizational culture through policies and derivative business processes.

The findings from my study highlight the complexity of developing and implementing employee privacy strategies. P1C stated that privacy was a "tricky" issue and that practitioners need to be mindful of the many aspects that need to be considered in developing and implementing a privacy program. I did not probe the participant on the use of "tricky" because I used the context and dictionary meaning to ascribe the meaning of "complex," and during member checking, the participant did not request any changes. My findings suggest that in practice, the approach to privacy has been hampered by the focus on personal information privacy. As such, the capabilities have not been expanded beyond administrative competencies, and leadership on employee/workplace privacy is scarce.

The findings from my study have verified the link between CLT, CT as presented by researchers such as Uhl-Bien (2021) and Baltaci and Balci (2017), and the employee/workplace privacy dimensions literature offered by researchers Ball et al.

(2013), Bhave et al. (2020), Igo (2022), and Katsabian (2020). This study has also linked organizational capabilities literature proposed by researchers such as Backlander (2019), Uhl-Bien (2021), and Wheatley (2011), with workplace/employee privacy literature, as the researchers suggested that humans/agents may change behaviors, demonstrate adaptive and enabling capabilities, and develop new policies and/or procedures in support of organizational change and development.

Because my findings reflect the dynamic capabilities needed for change to move beyond technological controls, to the valuing of employee privacy, through culture infusion, the findings illuminate a link between value-based decision making and employee/workplace privacy. Furthermore, my study's findings suggest a connection between human resources considerations literature in Ebert et al. (2021), the business and human and resources (BH&R) framework, and workplace/employee privacy dimensions as mentioned by researchers such as Ball et al. (2013), Bhave et al. (2020), and Smith et al. (2011).

Emergent Theme 2: Surveillance Capabilities (Autonomy Privacy)

Regarding the use of employee surveillance technologies, P1Cs stated, "We don't take advantage of that." P2Cs stated, "We don't use any surveillance tools on our end." The findings from my study suggest that the C-suite practitioners were managing the tensions noted in the literature by Bhave et al. (2020), Katsabian (2021), and Vegh (2018) between the need for organizational accountability and employee privacy. These practitioners were safeguarding employee privacy and managing for productivity without the overuse or abuse of surveillance technologies.

Autonomy privacy is a significant area of employee/workplace privacy and facilitates organizational performance aspects of creativity, problem solving, and productivity and enhances wellness and employee affective commitment. According to Mankins and Gortar (2017) and Mokrosinska (2018), autonomy could be viewed as socially embedded and the single most important element for creating employee engagement and well-being that yields creativity and innovation. The intrinsic value of privacy is essential and instrumental for thinking and acting freely (autonomy). However, unchecked autonomy without needed accountability can lead to organizational chaos. As such, Gierlich-Joas et al. (2022) provided suggestions for mitigating the tensions between transparency and employee privacy needs. The participants' responses suggest that both participants did not believe that their businesses' need to monitor productivity or performance required them to use surveillance capability at the risk of causing harm to their employees (autonomy privacy) and having an increase in turnover, along with reductions in creativity, problem solving, and organizational performance. The valuing of privacy allows for autonomy, which supports both organizational and individual wellness.

Emergent Theme 3: Predominant Focus on the Safeguarding of Personal Information (Personal Information Privacy) Using InfoSec Practices

The findings from my study corroborate those from Ball et al.'s (2013) research that not much practice is occurring on all the theoretically proposed dimensions of privacy, such as autonomy and environmental and personal information. P1Cs stated, "I think I've leaned very heavily on the technology tools." P2Cs stated, "We keep things off of the cloud and keep things locally stored, and password protected." The participants used information security protocols (InfoSec) and tools to safeguard specific data sets.

Currently, the practice of workplace/employee privacy management is primarily focused on personal information privacy, with reduced consideration for environmental privacy and autonomy. Environmental privacy is limited to the work-from-home (telework) policy. Care for the mental space (autonomy) is rarely mentioned, except in terms of surveillance and monitoring concerns.

I used a word search for the terms *personal information*, *autonomy*, and *environment* across the data sources that referenced personal information or some form across all data types and sources in this study. The findings suggested that many discussions within the literature revolve around the information management dimension of workplace privacy. As noted by Ball et al. (2013), not all three dimensions of employee/workplace privacy are being given equal weighting, even at this time.

For example, a word search across the data sources in my study for the "autonomy privacy" dimension was hardly mentioned beyond the academic literature. The word "autonomy" was not discussed in practice, but autonomy was discussed in terms of monitoring or surveillance. The word search across data sources in my study also highlighted that the phrase "environmental privacy" was only mentioned in the literature review source. In practice, physical and digital environmental privacy were discussed in terms of culture and valuing of employee privacy.

My findings suggest that the dimension of environmental privacy is represented as culture and valuing for the study's cases. However, the valuing of privacy, separation, segregation, architecting, authorized access, and minimal use of surveillance capabilities are all tactics that are being used for the safeguarding of employee privacy by these participants.

Applications to Professional Practice

My findings, conclusions, and recommendations could provide solutions to address small business leaders'/agents' need for suggested business design, practices, and strategies to safeguard employee privacy in their business, while providing revenues for supporting local economies. Business leaders/agents may use the findings from my study for (a) enhancing the design of their business model by infusing it with privacy consideration, to establish and retain trust, between employee and employer; (b) developing organizational strategies and programs; and (c) engaging CL tactics to safeguard employee/workplace privacy, reduce exposure and litigation risk, and sustain small businesses.

Small business owners may find the following themes of value in designing and implementing employee privacy strategies and processes: (a) an awareness of culture and value systems is necessary (environmental privacy), (b) surveillance capabilities are not currently being used by the C-suite leaders/agents (autonomy privacy), and (c) a predominant focus on the safeguarding of personal information assets using technological and InfoSec practices and policy controls (personal information privacy). I will provide the three participants with a summary of the published results and findings.

Implications for Social Change

The implications for positive social change include the potential for retaining productive employees and developing organizations that value privacy while also being profitable. This combination can result in increasing financial security for owners, employees, and employees' families, as well as financial support and employment opportunities for the local community. Additionally, this information might be useful for members of the chamber of commerce to share with owners of small businesses and for academia to instruct entrepreneurs on how to incorporate the valuing of workplace/employee privacy into their organizational designs.

Recommendations for Action

There is a high level of CL needed for the safeguarding of employee privacy. Five recommended actions for agents/leaders of small businesses to overcome barriers to developing and successfully implementing an employee/workplace privacy program are as follows:

1. Develop a comprehensive understanding of the value of employee privacy as both a human right and need and foster a culture and codevelop policies and operations around that. As stated by P1Cs, "I think the strategy of building the culture or awareness or training is needed." Agents/leaders of the SMBs may also establish privacy zones by getting employee privacy attitudes, concerns, and valuation inputs to develop collaborative policies that balance employer security and productivity concerns with employee privacy preferences. Such awareness and cocreation capabilities would support the generative and

emergent capability noted in complexity sciences and CLT, for micro, meso, and macro effects within an organization that can bring about changes in behaviors (Doyle, 2017; Hazy & Protas, 2018; Lichtenstein, 2020; Turner & Baker, 2019; Zimmerman, 2008). The development and use of the aforementioned capabilities would support the nature of complex adaptive systems, as many actors that exchange information mutually affect each other, and, in so doing, generate new valuing of behavior in specific areas that affect the system (Bryson et al., 2017; Horvat & Filipovic, 2018; Uhl-Bien, 2021).

2. Be courageous and lead in heralding strategic privacy by design in organizational designs. Establish the role of security in support of privacy. In my study, although some participants had policies, the policies focused only on information security (InfoSec) protocols for personal information and did not purposely address autonomy or environmental dimensions of employee privacy theory. This finding aligns with Ball et al.'s (2013) finding that there is a predominant focus on personnel information management.
3. Allocate funding for a robust privacy program that encompasses the three dimensions of personal information, autonomy, and environmental privacy and include privacy enhancing/enabled technologies and talent training. Train employees on various techniques and tools that they can use to safeguard their privacy—home/physical (environmental boundary), mental (autonomy), and personal information.

4. Design a program that contains both defensive and offensive safeguarding tactics. Defensive tactics may include informing employees on privacy technologies such as Abine, MySudo, BlackCloak, Cypient Black (Iannopollo & Shey, 2022), privacy.com, protonmail.com, Duck Duck GO, and Lifelock; principles; and practices. Offensive safeguarding tactics may include third-party and organizational accountability agreements for collecting, using, sharing, transferring, selling, and erasing employee data.
5. Establish partnerships with various privacy practitioners, legal and certified privacy, and organizational development consultants, to assist in the development and support of the privacy program. As stated by P1C,

> It is important to be aware of the legal and regional context of employee privacy and the sharing aspect. It's a very tricky area because it's tied to labor law. It's different for every country and every state. So, it's one of those areas where you must first look at what the rules are, but you have to more than likely, partner with local employment labor lawyers.

Recommendations for Further Study

My study's findings stem from its previously defined assumptions, limitations, and delimitations. Recommendations for further research include focusing on privacy practitioners – consultants (legal and business oriented), small business leaders/agents from varying levels of the organization, in different industries and varying geographical locations. Future researchers should also consider studying small business leaders/agents who demonstrate valuing privacy by appending a clear budget line item and have been profitable. Future researchers may also explore the relevance of the gender and age of the small business leaders/agents in developing and implementing workplace/employee privacy initiatives through quantitative and mixed-method designs. Moreover, focusing on each of the three specific themes identified within this study would provide more specific areas for additional research.

A cross study on ecommerce consumer privacy, private sector employee privacy, government employee privacy, dimensions, culture, regulations, expectations, limitations, boundaries, and theories, could provide richer insights into the landscape of privacy in the United States. Another area for future study may entail a literature review on workplace/employee privacy, consumer privacy and government employee privacy behaviors and privacy as a human right using Business & Human Resources lens (B&HR). A further area for research is to study employee beliefs about privacy in relation to their actual behaviors. For instance: Do employees seek to sustain their environmental privacy more than their information privacy? Do employees seek to sustain their autonomy more than their environmental privacy? Is any area of workplace privacy more significant than another? Are they all treated and held the same?

Another potential focus for further related research is to conduct studies on privacy enhancing technology (PET) in safeguarding employee privacy, for instance: What workplace privacy dimensions can privacy enhancing technologies affect? Do employees behave differently with their privacy dimensions in the real (physical) versus the digital world? If so, why, and when and if not, why not. For instance: Null

Hypothesis – Employees do not behave differently with their privacy in the real world than the digital world. Alternative Hypothesis - Employees behave differently with their privacy in the real world than in the digital world. Future research in such areas could help academia, business and government leaders provide improved support and resources to their local economy and communities through effective programs, business models and policies that provide for employee well-being, commitment, innovation, and productivity.

Reflections

During my time in the Walden DBA program, I explored multiple possible research questions such as disaster recovery and technology adoption management in SMBs. In 2019, I ultimately selected privacy and specifically employee/workplace privacy since based upon my exploratory research, it was the least mentioned aspect at the time. The COIVD-19 pandemic though, created a confluence such that virtual and physical boundaries were being redefined, and trust and productivity had to harmonize during the early stages, for work to be done. Employee/workplace privacy concerns in relation to personal information was heightened. The dimensions of autonomy and environmental employee privacy, in this era of the digitization of the workplace and remote work design, are being revisited. Furthermore, Bloustein's (2018) notions of individual and group privacy, as a factor of human dignity and security of social freedoms are also being revisited.

Through a substantive literature review, engagements in the privacy arena, and my opportunity to gather evidence from my privacy practitioners - small business leaders/agent participants, I have developed a better understanding of the notion and treatment of employee/workplace privacy in the United States. I struggled to get certified privacy practitioners, who could speak beyond the personal information dimension of workplace/employee privacy, to participate in the study. However, over time, with socializing and patience, my professional network responded with three qualified participants, and I was able to glean much from their responses, and I am grateful for their time with me.

Designing and implementing this study has enlightened me in numerous ways: (a) how to align the research question with the methodology and design, (b) how to use the literature to expand my knowledge and set a priori baseline, (c) how to conduct interviews, and (d) how to collect, organize, analyze (e.g., developing codes, conducting methodological triangulation) visualizing and summarizing results (word clouds, matrices, word trees, and graphs) and interpreting data using both manual and computer-aided techniques.

Study Conclusions

The purpose of this qualitative multiple case study was to explore the strategies small business leaders/agents use to safeguard employee privacy. The population for this study was three small business leaders/agents, (privacy practitioners) who have effectively safeguarded employee/workplace privacy, in the Mid-Atlantic region of the United States. As such, this study is not be generalizable. However, I have attempted to provide sufficient information for the reader to determine its transferability.

As described by Fusch (2017) and Saunders et al. (2018), I concluded data saturation was reached when no new information emerged after member checking and analysis across the five data sources - P1C, P1Cs, P2Cs, privacy blog, and published employee privacy policies. After I coded and analyzed the data, three major themes emerged: (a) an awareness of culture and value systems is necessary (environmental privacy), (b) surveillance capabilities are not currently being used by the C-suite leaders/agents (autonomy privacy), (c) a predominant focus is on the safeguarding of personal information assets using technological and information security (InfoSec) practices and policy controls (personal information privacy).

References

Abrams, M., Abrams, J., Cullen, P., & Goldstein, L. (2019). Artificial intelligence, ethics, and enhanced data stewardship. *IEEE Security & Privacy, Security & Privacy, 17*(2), 17–30. https://doi.org/ 10.1109/MSEC.2018.2888778

Adams, M. 2017. Big data and individual privacy in the age of the Internet of Things. *Technology Innovation Management Review, 7*(4), 12–24. https://doi.org/10.22215/timreview/1067

Agarwal, A. K., Gans, J. S., & Goldfarb, A. 2017. What to expect from artificial intelligence? *MIT Sloan Management Review, 58*(3), 23–27. https://doi.org/10.7551/mitpress/11645.003.0008

Ahern, K. J. (1999). Ten tips for reflexive bracketing. *Qualitative Health Research*, *9*(3), 407–411. https://doi.org/10.1177/104973239900900309

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extrarole performance. *Journal of Applied Psychology, 91*(1), 221–232. https://doi.org/ 10.1037/0021-9010.91.1.221

Aluwihare-Samaranayake, D. (2012). Ethics in qualitative research: A view of the participants' and researchers' world from a critical standpoint. *International Journal of Qualitative Methods, 11*(2), 64–81. https://doi.org/10.1177/160940691201100208

Anciaux, N., Bonnet, P., Bouganim, L., Nguyen, B., Pucheral, P., Sandu Popa, I., & Scerri, G. (2019). Personal data management systems: The security and functionality standpoint. *Information Systems*, *80*, 13–35.

https://doi.org/10.1016/j.is.2018.09.002

Apare, R. S., & Gujar, S. (2018). Research issues in privacy preservation in IoT. In *2018 IEEE Global Conference on Wireless Computing and Networking* (pp. 87–90). IEEE. https://doi.org/10.1109/GCWCN.2018.8668616

Areheart, B., & Roberts, J. (2019). GINA, Big Data, and the future of employee privacy. *Yale Law Journal*, *128*(3), 710–790.

Arnaud, S., & Chandon, J. L. (2013). Will monitoring systems kill intrinsic motivation? An empirical study. *Human Resources Management Review*, *90*(4), 35–53. https://doi.org/10.3917/GRHU.090.0035

Asbari, M. (2020). Is transformational leadership suitable for future organizational needs*? International Journal of Social, Policy and Law, 1*(1), 51–55. https://doi.org/ 10.8888/ijospl.v1i1.17

Bäcklander, G., (2019). To see or not to see: Importance of sensemaking in employee self-direction. *Nordic Journal of Working Life Studies, 9*(2), 25–45. https://doi.org/10.18291/njwls.v9I2.114799

Ball, K., Daniel, E. M., & Stride, C. (2013). Dimensions of employee privacy: An empirical study. *Information Technology & People*, *25*(4), 376–394. https://doi.org/10.1108/09593841211278785

Baltacı, A., & Balcı, A. (2017). Complexity leadership: A theoretical perspective. *International Journal of Educational Leadership and Management, 5*(1), 30–59. https://doi.org/10.17583/ijelm.2017.2435

Bearss, K., Taylor, C. A., Aman, M. G., Whittemore, R., Lecavalier, L., Miller, J., Pritchett, J., Green, B., & Scahill, L. (2016). Using qualitative methods to guide scale development for anxiety in youth with autism spectrum disorder. *Autism, 20*(6), 663–672. https://doi.org/10.1177/1362361315601012

Beehner, C. G. (2019). *System leadership for sustainability*. Routledge.

Benmira, S., & Agboola, M. (2021). Evolution of leadership theory. *BMJ Leader*, *5*(1), 3–5. https://doi.org/10.1136/leader-2020-000296

Bhave, P., Teo, H., & Dalal, S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, *46*(1), 127–164. https://doi.org/10.1177/0149206319878254

Bloustein, E. J. (2018). *Individual & group privacy*. Routledge.

Boatwright, C. B., & White, C. (2020). Is privacy dead? Does it matter? *Journal of Public Interest Communications, 4*(1), 78–101. https://doi.org/10.32473/jpic.v4.i1.p78

Bodie, M. T. (2022). The law of employee data: Privacy, property, governance. *Indiana Law Journal*, *97*, 1–67. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3819897

British Broadcasting Company. (2017, October 6). *Is privacy dead in an online world?* https://www.bbc.com/news/technology-41483723

Bryson, J., Sancino, A., Benington, J., & Sørensen, E. (2017). Towards a multi-actor theory of public value co-creation. *Public Management Review, 19*(5), 640–665. https://doi.org/10.1080/14719037.2016.1192164

Burcharth, A., Knudsen, M. P., & Søndergaard, H. A. (2017). The role of employee autonomy for open innovation performance. *Business Process Management Journal*, *6*(23), 1245–1269. https://doi.org/10.1108/BPMJ-10-2016-0209

Byers, V. T., Smith, R. N., Hwang, E., Angrove, K. E., Chandler, J. I., Christian, K. M., Dickerson, S. H., McAlister-Shields, L., Thompson, S. P., Denham, M. A., & Onwuegbuzie, A. J. (2014). Survival strategies: Doctoral students' perceptions of challenges and coping methods. *International Journal of Doctoral Studies*, *9*, 109–136. https://ijds.org/Volume9/IJDSv9p109-136Byers0384.pdf

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, *25*(8), 652–661. https://doi.org/10.1177/1744987120927206

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811–831. https://www.proquest.com/scholarly-journals/preparing-interview-research-protocol-refinement/docview/1806967398/se-2

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019

Cavoukian, A., & Chibba, M. (2018). Start with privacy by design in all big data applications. In: S. Srinivasan, (Ed.) *Guide to big data applications. Studies in big data, 26.* Springer, Cham. https://doi.org/ 10.1007/978-3-319-53817-4_2

Cha, S. C., Hsu, T. Y., Xiang, Y., & Yeh, K. H. (2019). Privacy enhancing technologies in the internet of things: Perspectives and challenges. *IEEE Internet of Things Journal, 6*(2), 2159–2187. https://doi.org/10.1109/JIOT.2018.2878658

Cheng, S., Delmar, F., & Croidieu, G. (2020). The "Emergence" of new organizations - A complex adaptive systems perspective. *Academy of Management Annual Meeting Proceedings, 2020*(1), Article 14031. https://doi.org/10.5465/AMBPP.2020.14031abstract

Chibba, M., & Cavoukian, A. (2018). Privacy, consumer trust and big data: Privacy by design and the 3c's. Privacy and Big Data Institute, Ryerson University, Toronto, Canada. https://doi.org/10.1109/Kaleidoscope.2015.7383624

Childress, J. F., & Beauchamp, T. L. (2022). Common morality principles in biomedical ethics: Responses to critics. *Cambridge Quarterly of Healthcare Ethics, 31*(2), 164-176. https://doi.org/10.1017/S0963180121000566

Choi, H. S., Lee, W. S., & Sohn, S. Y. (2017). Analyzing research trends in personal information privacy using topic modeling. *Computers & Security*, *67(June)*, 244–253. https://doi.org/10.1016/j.cose.2017.03.007

Claiming Human Rights (2018). Article 12. https://www.claiminghumanrights.org

Cook, K. D. (2017). *Effective cybersecurity strategies for small businesses*. (Order No. 3871). [Doctoral Dissertation, Walden University*]*. https://scholarworks.waldenu.edu/dissertations/3871/

Cortini, M., & Fantinelli, S. (2018). Fear for doxing and digital privacy in the workplace: A dual pathway model. *Management Revue*, *29*(2), 162–178. https://doi.org/10.5771/0935-9915-2018-2-162

Coss, D.L. and Dhillon, G. (2019), Cloud privacy objectives a value based approach. *Information and Computer Security, 27*(2). 189–220. https://doi.org/10.1108/ICS-05-2017-0034

Crane, A., Henriques, I., & Husted, B. W. (2018). Quants and poets: Advancing methods and methodologies in business and society research. *Business & Society, 57*(1), 3–25. https://doi.org/10.1177/0007650317718129

Craps, M., Vermeesch, I., Dewulf, A., Sips, K., Termeer, K., & Bouwen, R. (2019). A relational approach to leadership for multi-actor governance. *Administrative Sciences 9*(1), 2764–2776. https://doi.org/10.3390/admsci9010012

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, *21*(5), 19–27. https://doi.org/10.7748/nr.21.5.19.e1240

Cronk, J. (2018). *Strategic privacy by design.* International Association of Privacy Professionals (IAAP) Publishing.

Crozier, S. E., & Cassell, C. M. (2016). Methodological considerations in the use of audio diaries in work psychology: Adding to the qualitative toolkit. *Journal of Occupational and Organizational Psychology*, *89*(2), 396–419. https://doi.org/10.1111/joop.12132

Cypress B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing: DCCN*, *36*(4), 253–263.

https://doi.org/10.1097/DCC.0000000000000253

Deakin, H., & Wakefield, K. (2014). Skype interviewing: Reflections of two PhD researchers. *Qualitative Research, 14*(5), 603–616. https://doi.org/10.1177/1468794113488126

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research, 6*(2), 80-88. https://doi.org/10.1177/1558689812437186

Dhillon, G., Oliveira, T., & Syed, R. (2018). Value-based information privacy objectives for Internet Commerce. *Computers in Human Behavior*. *87*, 292–307. https://doi.org/10.1016/j.chb.2018.05.043

Dobson, J.E., & Herbert, W.A. (2021). Geoprivacy, convenience, and the pursuit of anonymity in digital cities. In W. Shi, M.F. Goodchild, M. Batty, M., MP. Kwan, A. Zhang. (Eds.), *Urban Informatics,* pp. 567–587. The Urban Book Series. Springer. https://doi.org/10.1007/978-981-15-8983-6_32

Doyle, A. (2017). Adaptive challenges require adaptive leaders. *Performance Improvement*, *56*(9), 18–26. https://doi.org/10.1002/pfi.21735

Dragano, N., & Lunau, T. (2020). Technostress at work and mental health: Concepts and research results, *Current Opinion in Psychiatry 33*(4). 407–413. https://doi.org/10.1097/YCO.0000000000000613

Ebert, I., Wildhaber, I., & Adams-Prassl, J. (2021). Big Data in the workplace: Privacy due diligence as a human rights-based approach to employee privacy protection. *Big Data & Society, 8*(1), 1–14. https://doi.org/10.1177/20539517211013051

Edwards-Brown, L. (2020). *Successful strategies to lead change initiatives*. (Order No. 8028). [Doctoral Dissertation, Walden University]. https://scholarworks.waldenu.edu/dissertations/8028

Erlingsson, C., & Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, *7*(3), 93–99. https://doi.org/10.1016/j.afjem.2017.08.001

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1– 4. https://doi.org/10.11648/j.ajtas.20160501.11

Fairclough, B. (2016). Privacy piracy: The shortcomings of the United States' data privacy regime and how to fix it. *Journal of Corporation Law*, *42*(2), 461– 480. https://jcl.law.uiowa.edu

Federal Trade Commission. (2018). *Protecting personal information: A guide for businesses*. https://business.ftc.gov

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a miniethnographic case study: A guide for novice researchers. *The Qualitative Report, 22*(3) 923–941. https://nsuworks.nova.edu/tqr/vol22/iss3/16

Gierlich-Joas, M., Teebken, M., & Hess, T. (2022, January). *A synthesized perspective on privacy and transparency in the digital workplace.* [Presentation Paper]. In Proceedings of the 55th Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2022.633

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care*

Chaplaincy, 20(3), 109–122. https://doi.org/10.1080/08854726.2014.925660

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. *Academy of Business, Engineering and Science, 12*(1), 1–12. https://www.academia.edu/38674702

Hallett, R. E., & Barber, K. (2014). Ethnographic research in a cyber era. *Journal of Contemporary Ethnography, 43*(3), 306–330. https://doi.org/10.1177/0891241613497749

Harley, B., & Cornelissen, J. (2022). Rigor with or without templates? The pursuit of methodological rigor in qualitative research. *Organizational Research Methods, 25*(2), 239–261. https://doi.org/10.1177/1094428120937786

Hazy, J. K., & Prottas, D. J. (2018). Complexity leadership: Construct validation of an instrument to assess generative and administrative leadership modes. *Journal of Managerial Issues, 30*(3), 325–277. 107119_JMI text.indd (researchgate.net)

Hertel, G., Stone, D. L., Johnson, R. D., & Passmore, J. (2017). The psychology of the Internet @ work. In G. Hertel, D. L. Stone, R. D. Johnson, & J. Passmore (Eds.), Wiley Blackwell handbooks in organizational psychology. The Wiley Blackwell handbook of the psychology of the Internet at work (pp. 1–18). Wiley Blackwell. https://doi.org/10.1002/9781119256151.ch1

Hieker, C., & Pringle, J. (2020). *The Future of Leadership Development: Disruption and the Impact of Megatrends*. Springer Nature.

Hoepman, J.H. (2018). *Privacy design strategies*. IFIP International Information Security Conference. 446–459. https://doi.org/10.1007/978-3-642-55415-5_38

Hornberger, R. C (2021). Creating a sense of digital privacy in the private sector. *Information Security Journal: A Global Perspective, 30*(1), 30–56. https://doi.org/10.1080/19393555.2020.1797948

Horvat, A., & Filipovic, J. (2018). Service quality and maturity of health care organizations through the lens of complexity leadership theory. *Journal of Evaluation in Clinical Practice, 24*(1), 301–307. https://doi.org/10.1111/jep.12789

Iannopollo, E., & Shey, H., (2022, January 28). The future of work: Employee privacy. Forrester. https://www.forrester.com/blogs/the-future-of-work-employee-privacy/

Igo, S. E. (2018). *The known citizen.* Harvard University Press.

Igo, S. E. (2022). Privacy isn't dead. *Atlantic, 329*(4), 80–84. https://www.magzter.com/stories/News/The-Atlantic/Privacy-Isnt-Dead

International Organization for Standards. (n.d). ISO/IEC 29100:2011(en). Information technology — Security techniques — Privacy framework. https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en

Janghorban, R., Roudsari, R. L., & Taghipour, A. (2014). Skype interviewing: The new generation of online synchronous interview in qualitative research. *International Journal of Qualitative Studies on Health and Well-Being*, *9*(1). 1–3 https://doi.org/10.3402/qhw.v9.24152

Jansson, N. (2013). Organizational change as practice: A critical analysis. *Journal of Organizational Change Management 26*(6). 1003–1019. https://doi.org/10.1108/JOCM-09-2012-0152

Jervis, C. E. M. (2018). Barbulescu v Romania: Why there is no room for complacency when it comes to privacy rights in the workplace. *Industrial Law Journal*, *47*(3), 440–453. https://doi.org/10.1093/indlaw/dwy002

Jiang, H., Tsohou, A., Siponen, M., & Li, Y. (2020). Examining the side effects of organizational internet monitoring on employees. *Internet Research, 30*(6), 1613–1630. https://doi.org/ 10.1108/intr-08-2019-0360

Jovanović, P., & Božičić, M. (2018). Employee's right to privacy as an essential part of decent work. *University of Novi Sad, Faculty of Law, 52*(3), 855–868. https://doi.org/10.5937/ZRPFNS52-20000

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

Katsabian, T., (2020). The Telework Virus: How the COVID-19 pandemic has affected telework and exposed its implications for privacy and equality. *The Social Sciences Repository Network (SSRN)*. 1–55. https://doi.org/10.2139/ssrn.3684702

Katsabian, T., (2019). Employees' privacy in the internet age: Towards a new procedural approach. *Berkeley Journal of Employment and Labor Law, 40*(2). 203–255. https://doi.org/10.15779/Z38NG4GS3G

Kay, N. M., Leih, S., & Teece, D. J. (2018). The role of emergence in dynamic capabilities: A restatement of the framework and some possibilities for future research. *Industrial and Corporate Change, 27*(4), 623–638.

https://doi.org/10.1093/icc/dty015

Keshu, L., & Meixia, S. (2020). Personal information security crisis in the era of big data. *Journal of Physics Conference Series, 1486*(5), 1–8. https:/doi.org/10.1088/1742-6596/1486/5/052002

Kirk, N. (2018). Compliance and personal data protection: The EU is getting serious about data protection via the GDPR. *Journal of Property Management, 83*(3), 40–42. https://www.irem.org/resources/jpm.

Kshetri, N., & DeFranco, J. F. (2020). Is privacy dead? *IT Professional, 22*(5), 4–12. https://doi.org/10.1109/MITP.2020.2992148

Kyngäs, H., Kääriäinen, M., & Elo, S. (2020). The trustworthiness of content analysis. In *The application of content analysis in nursing science research* (pp. 41–48). Springer. https://doi.org/10.1007/978-3-030-30199-6_5

Lester, G. V., Palanski, M., Hammond, M., & Clapp-Smith, R. (2017). Multi-domain leadership: A whole person approach to leading in the workplace . . . and beyond. *Organizational Dynamics, 46*(3), 133–139. https://doi.org/10.1016/j.orgdyn.2016.11.001

Leung L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324–327. https://doi.org/10.4103/2249-4863.161306

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation and Program Planning, 68(June),* 157–165.

https://doi.org/10.1016/j.evalprogplan.2018.03.005

Li, C., & Palanisamy, B. (2018). Privacy in internet of things: From principles to technologies. *IEEE Internet of Things Journal*, *6*(1), 488–505. https://doi.org/10.1109/JIOT.2018.2864168

Lichtenstein, B. (2020). Generative emergence: Research and praxis for social innovation. *Oxford Research Encyclopedia of Psychology.* https://doi.org/10.1093/acrefore/9780190236557.013.735

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Lo Iacono, V., Symonds, P., & Brown, D.H. (2016). Skype as a tool for qualitative research interviews. *Sociological Research Online, 21*(2), 103–117. https://doi.org/10.5153/sro.3952

Lorinkova, N. M., & Bartol, K. M. (2021). Shared leadership development and team performance: A new look at the dynamics of shared leadership. *Personnel Psychology, 74*(1), 77–107. https://doi.org/10.1111/peps.12409

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education, 9*(3). 3351–33514. https://ojs.aishe.org/index.php/aishe-j/article/view/335/553

Mankins, M., & Garton, E. (2017). How Spotify balances employee autonomy and accountability. *Harvard Business Review*, *95*(1). 134–139. https://hbr.org/2017/02/how-spotify-balances-employee-autonomy-and-accountability

Marchiori, D., & Mendes, L. (2018). Knowledge management and total quality management: Foundations, intellectual structures, insights regarding evolution of the literature. *Total Quality Management & Business Excellence, 31*(9/10), 1135–1169. https://doi.org/10.1080/14783363.2018.1468247

Marshall, C., & Rossman, B. G. (2016). *Designing qualitative research*, (6th ed.). Sage.

Mathews, K. M., White, M. C., & Long, R. G. (1999). Why study the complexity sciences in the social sciences? *Human Relations, 52(*4), 439–462. https://doi.org/10.1177/001872679905200402

Matt, M., Gaunand, A., Joly, P.-B., & Colinet, L. (2017, February 1). Opening the black box of impact -- Ideal-type impact pathways in a public agricultural research organization. *Research Policy, 46*(1), 207–218. https://doi.org/10.1016/j.respol.2016.09.016

Mayoh, J., & Onwuegbuzie, A. J. (2015). Toward a conceptualization of mixed methods phenomenological research. *Journal of Mixed Methods Research*, *9*(1), 91–107. https://doi.org/10.1177/1558689813505358

McParland C., & Connolly R. (2020). Dataveillance in the workplace: Managing the impact of innovation. *Business Systems Research*, *11*(1), 106–124. https://doi.org/10.2478/bsrj-2020-0008

Miller, D., & Slater, D. (2020). *The Internet: An ethnographic approach*. Routledge.

Mims, C. (2018). Privacy is dead. Here's what comes next. *Wall Street Journal*. https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001

Mokrosinska, D. (2018). Privacy and autonomy: On some misconceptions concerning the political dimensions of privacy. *Law and Philosophy, 37*(2), 117–143. https://doi.org/10.1007/s10982-017-9307-3

National Institute of Science and Technology, 2022. *NIST Cybersecurity & Privacy Annual Report - FY2020*. https://doi.org/ 10.6028/NIST.SP.800-214

Nortey, R.N., Yue, L., Agdedanu, P., R. & Adjesisah, M. (15-18 March 2019). *Privacy module for distributed electronic health records (EHRs) Using the Blockchain*. [Paper presentation]. IEEE 4th International Conference on Big Data Analytics *(ICBDA*), 369–374. https://doi.org/10.1109/ICBDA.2019.8713188

Ngozwana, N. (2018). Ethical dilemmas in qualitative research methodology: Researcher's reflections. *International Journal of Educational Methodology*, *4*(1), 19–28. https://doi.org/10.12973/ijem.4.1.19

Olteanu, A. (2019). *Interdependent and multi-subject privacy: Threats, analysis, and protection.* EPFL. https://doi.org/10.5075/epfl-thesis-9373

Ospina, S. M., Foldy, E. G., Fairhurst, G. T., & Jackson, B. (2020). Collective dimensions of leadership: Connecting theory and method. *Human Relations, 73*(4), 441–463. https://doi.org/10.1177/0018726719899714

Pacho, Titus. (2015). Exploring participants' experiences using case study. *International Journal of Humanities and Social Science. 5(4)*. 44–53. https://www.researchgate.net/publication/280134008_Exploring_Participants%27_Experiences_Using_Case_Study

Pappas, I.O., Mikalef, P., Giannakos, M.N., Krogstie, J., & Lekakos, G. (2018). Big data and business analytics ecosystems: Paving the way towards digital transformation and sustainable societies. *Inf Syst E-Bus Manage 16***,** 479–491. https://doi.org/10.1007/s10257-018-0377-z

Pervez, S., Naher, S., Pranta, M. U. R., Banik, R., & Rahman, Q. M. (2021). Perception and experiences regarding COVID-19 pandemic among urban young adults in Bangladesh: A mixed-method study. *Journal of Public Health*, PMCID: PMC8236738. 1–11. https://doi.org/10.1007/s10389-021-01600-3

Pierre-Francois, W., & Guzman, I. (2020). Factors that influence HIPAA Secure compliance in small and medium-size health care facilities. https://digitalcommons.keenesaw.edu/ccerp/2020/Research/6

Poleto, T., Clemente, T.R.N., de Gusmão, A.P.H., Silva, M.M. & Costa, A.P.C.S. (2020), Integrating value-focused thinking and FITradeoff to support information technology outsourcing decisions, *Management Decision, 58*(11), 2279–2304. https://doi.org/10.1108/MD-09-2019-1293

Prakke H, & Wurster J. (1999). Quality criteria for qualitative research. *Pflege. 12*(3), 183 –186. https://doi.org/10.1024/1012-5302.12.3.183

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies 3*(9). 369–387. https://doi.org/10.5281/zenodo.887088.

Rant, M. B. (2020). Sustainable development goals (SDGs), leadership, and Sadhguru: Self-transformation becoming the aim of leadership development. *The International Journal of Management Education, 18*(3), Article 100426. https://doi.org/10.1016/j.ijme.2020.100426

Rath, D.K., & Kumar, A. (2021). Information privacy concern at individual, group, organization, and societal level - a literature review. *Vilakshan - XIMB Journal of Management*, *18*(2). 171–186. https://doi.org/10.1108/XJM-08-2020-0096

Riveni, Hillen, & Dustdar, (15-17 Dec. 2017). *A toll data publishing method using encryption and differential privacy preservation technology*. [Presentation Paper]. IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 1586. https://doi.org/10.1109/ITNEC.2017.8285062

Rosenhead, J., Franco, L. A., Grint, K., & Friedland, B. (2019). Complexity theory and leadership practice: A review, a critique, and some recommendations. *The Leadership Quarterly, 30*(5). Article 101304. https://doi.org/10.1016/j.leaqua.2019.07.002

Ruiner, C., & Klumpp, M. (2022). Autonomy and new modes of control in digital work contexts – a mixed-methods study of driving professions in food logistics. *Employee Relations, 44*(4). 890–912. https://doi.org/10.1108/ER-04-2021-0139

Safonov, Y., Maslennikov, Y., & Lenska, N. (2018). Evolution and modern tendencies in the theory of leadership. *Baltic Journal of Economic Studies, 4*(1), 304–310. https://doi.org/10.30525/2256-0742/2018-4-1-304-310

Sarmah, P., Van den Broeck, A., Schreurs, B., Proost, K., & Germeys, F. (2022). Autonomy supportive and controlling leadership as antecedents of work design and employee well-being. *BRQ Business Research Quarterly*, *25*(1), 44–61.

https://doi.org/10.1177/23409444211054508

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Saunders, M.N.K., Lewis, P. & Thornhill, A. (2019) *Research methods for business students*. (8th ed.). Pearson.

Saunders, M. N. K., & Townsend, K. (2016). Reporting and justifying the number of interview participants in organization and workplace research. *British Journal of Management*, *27*(4), 836–852. https://doi.org/10.1111/1467-8551.12182

Scarpenellini, S., Marín-Vinuesa, L. M., Aranda-Usón, A., & Portillo-Tarragona, P. (2020). Dynamic capabilities and environmental accounting for the circular economy in businesses. *Sustainability Accounting, Management and Policy Journal, 11*(7), 1129–1158. https://doi.org/10.1108/SAMPJ-04-2019-0150

Schneider, A., Wickert, C., & Marti, E. (2017). Reducing complexity by creating complexity: A systems theory perspective on how organizations respond to their environments. *Journal of Management Studies, 54*(2), 182–208. https://doi.org/10.1111/joms.12206

Sengupta, S. S. (2019). Creating value-based organizational environment through integral leadership. *IUP Journal of Organizational Behavior*, *18*(2), 7–24. ISSN: 1948-0733.

Shipman, A., & Watkins, S. (2019). *ISO/IEC 27702:2019. An introduction to Privacy*

Information Management. IT Governance Press.

Shufutinsky, A. (2020). Employing use of self for transparency, rigor, trustworthiness, and credibility in qualitative organizational research methods. *Organization Development Review*, *52*(1), 50–58. https://www.researchgate.net/publication/340539936_Employing_Use_of_Self_for_Transparency_Rigor_Trustworthiness_and_Credibility_in_Qualitative_Organizational_Research_Methods

Simon, M. (2011). *Dissertation and scholarly research: Recipes for success.* Dissertations Success.

Simpson, M. (2018). *Complexity theory of leadership and management information* [Walden Dissertations and Doctoral Studies]. (Order No. 6121). https://scholarworks.waldenu.edu/dissertations/6121

Singh, S., & Kumar, D. (26-28 Feb. 2020). *Perceptions of security and privacy in Internet of Things.* [Presentation paper]. 2020 International Conference on Inventive Computation Technologies (ICICT), 810–813. https://doi.org/10.1109/ICICT48043.2020.9112462

Smith, S. A., & Brunner, S. R. (2017). To reveal or conceal: Using communication privacy management theory to understand disclosures in the workplace. *Management Communication Quarterly, 31*(3), 429–446. https://doi.org/10.1177/0893318917692896

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: Problems and opportunities within sport and exercise psychology. *International*

Review of Sport and Exercise Psychology, 11(1), 101–121. https://doi.org/10.1080/1750984X.2017.1317357

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *Management Information Systems - Quarterly, 35*(4), 989–1015. https://doi.org/10.2307/41409970

Stake, R. E. (2013). *Multiple case studies*. Guilford press.

Tarafdar, M., Cooper, C. L., & Stich, J. F. (2019). The technostress trifecta-techno eustress, techno distress and design: Theoretical directions and an agenda for research. *Information Systems Journal*, *29*(1), 6–42. https://doi.org/10.1111/isj.12169

Teebken, M., & Hess, T. (2021, January 5). *Privacy in a digitized workplace: Towards an understanding of employee privacy concerns* [Conference session]. 54th Hawaii International Conference on System Sciences. Hawaii, United States. https://doi.org/10.24251/HICSS.2021.800

Teebken, M. (2021, August 9). *What makes workplace privacy special? An investigation of determinants of privacy concerns in the digital workplace.* [Paper presentation]. Americas Conference on Information Systems (AMCIS). https://www.researchgate.net/publication/352569537_What_Makes_Workplace_Privacy_Special_An_Investigation_of_Determinants_of_Privacy_Concerns_in_the_Digital_Workplace

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative Nursing-Quarterly*, *7*(3), 155–163.

https://doi.org/10.5281/zenodo.2552022

Tomczak, D., Lanzo, L., & Aguinis, H. (2018). Evidence-based recommendations for employee performance monitoring. *Business Horizons, 61*(2), 251–259. https://doi.org/10.1016/j.bushor.2017.11.006

Tourish, D. (2019). Is complexity leadership theory complex enough? A critical appraisal, some modifications, and suggestions for further research. *Organization Studies, 40*(2), 219–238. https://doi.org/10.1177/0170840618789207

Turner, J. R., & Baker, R. M. (2019). Complexity theory: An overview with potential applications for the social sciences. *Systems*, *7*(1), 1–22. https://doi.org/10.3390/systems7010004

Turner, W. (2020). Chipping away at workplace privacy: The implantation of RFID microchips and erosion of employee privacy. *Washington University Journal of Law & Policy*, *61*(1), 275–298. https://openscholarship.wustl.edu/law_journal_law_policy/vol61/iss1/18/

Tewes, E, 2017. #Privatesphere: Can privacy laws adequately protect employees amidst the complexities of the modern employment relationship? Santa Clara Law Review, 57(1), 287–312. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2839&context=lawreview

Uhl-Bien, M. (2021). Complexity leadership and followership: Changed leadership in a changed world. *Journal of Change Management*, *21*(2), 144–162. https://doi.org/10.1080/14697017.2021.1917490

United Nations, (2012). Global pulse on big data for development. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://unglobalpulse.org/wp-content/uploads/2012/05/BigDataforDevelopment-UNGlobalPulseMay2012.pdf

Ury, W. (2017). Mr. positive sum. *Negotiation Journal, 33*(4), 355–357. https://doi.org/10.1111/nejo.12198

van Manen, M., & van Manen, M. (2021). Doing phenomenological research and writing. *Qualitative Health Research, 31*(6), 1069–1082. https://doi.org/10.1177/10497323211003058

Vegh, L. (2018). *A survey of privacy and security issues for the Internet of Things in the GDPR Era*. [Conference session]. International Conference on Communications (COMM)*,* 453–458. https://doi.org/10.1109/ICComm.2018.8453643

Voss, C. A. (2017). *The narrative journey of the conscious leader* (Order No. 10587814). Available from ProQuest Dissertations & Theses Global. (1886084998).

Walsh, D., Parisi, J. M., & Passerini, K. (2017). Privacy as a right or as a commodity in the online world: The limits of regulatory reform and self-regulation*. Electronic Commerce Research, 17*(2), 185–203. https://doi.org/10.1007/s10660-015-9187-2

Warren, S., & Bandeis, L., (1860). The right to privacy. *Harvard Law Review, 4*(5).193–220. https://links.jstor.org/sici?sici=0017811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C

Weber, C. Gatersleben, B. Degenhardt, B. & Windlinger, L. (2021). *Privacy regulation theory: Redevelopment and application to workplace privacy.* Routledge.

https://doi.org/10.1201/9781003128830-6

Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 1–558. https://scholarlycommons.law.wlu.edu/wlulr

Westin, A. F. (1996). Privacy in the workplace: How well does American law reflect American values? *Chicago-Kent Law Review, 72*(1), 271–279. https://www.kentlaw.iit.edu

Wheatley. M. (2011). *Leadership and the new science: Discovering order in a chaotic world*. Berrett-Khoeler.

Wheatley, M. (2017). *Who do we choose to be? Facing reality, claiming leadership, restoring sanity.* Berrett-Khoeler.

Xianmang H., Yuan H., & Yindong C., (2018). Exploring the privacy bound for differential privacy: From theory to practice. *EAI Endorsed Transactions on Security & Safety, 5*(18), 1–11. https://doi.org/10.4108/eai.8-4-2019.157414

Yin, R. K. (2018). *Case study research and applications: Design and method* (6th ed.). Sage publications.

Zhu, J., Liao, Z., Yam, K. C., & Johnson, R. E. (2018). Shared leadership: A state-of-the-art review and future research agenda. *Journal of Organizational Behavior, 39*(7), 834–852. https://doi.org/10.1002/job.2296

Zilber, T. B. (2020). The methodology/theory interface: Ethnography and the microfoundations of institutions. *Organization Theory, 1*, 1–27. https://doi.org/10.1177/2631787720919439

Zimmerman, B., Linderberg, C., & Pisek, P. (2008). *Lessons from complexity science for* *health care leaders.* Edgeware.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

Appendix A: Recruitment E-Flyer

"Qualitative Study Researcher seeking privacy practitioners who are employed by or consulting on the safeguarding of employee privacy, in small to midsized organizations in the Mid-Atlantic region of the United States of America."
(Open for four weeks)

There is a new study called *"Safeguarding Employee Privacy in US based Small and Medium sized businesses"* that could help business practitioners better understand the privacy concerns of their employees and develop adequate solutions. For this study, privacy practitioners - consultants, C-Suite and mid-level managers, are invited to describe their experiences. Each volunteer will receive a $20 US e-gift card for completing the study, even if they do not answer all the interview questions.

The interviews are part of the doctoral study for Kim de Peiza, a Doctor of Business Administration (DBA) student at Walden University.

About the study:

- One 30-minute virtual audio recorded interview (phone in option available)
- One 30-minute member checking for interpretation agreement (web-based recorded - phone in option available)

To protect your privacy, no organization, or participants names will be reflected in the final study.

Volunteers must meet these requirements:

- 18+ years old
- History of developing and implementing successful strategies and processes for employee privacy management, employee information management or data governance.
- Either practicing/practiced in and Small or Medium sized Business in the Mid-Atlantic region of the United States of America.

Volunteers can ONLY participate if they meet the inclusion criteria for the study.

If you meet this inclusion criteria, and you are interested in participating in this study, please contact the researcher Kim de Peiza at kim.depeiza@waldenu.edu

N.B. All volunteers, who meet the inclusion criteria, may NOT be included in the study due to study parameters and data saturation.
All participants accepted into the study are eligible to receive study results. They may opt for either a 1-2-page result summary or a 15 mins verbal presentation of study results.

Appendix B: Participant Recruitment Letter

Date:
Subject: Request to Participate in a Research Study

Dear (Recipient):

I am a student at Walden University pursuing a Doctor of Business Administration (DBA) degree. You might already know me as a management consultant, but this study is separate from that role**.** I am conducting a research study on employee privacy for small and medium businesses (SMB) owners in the Northeastern region of the United States of America. The title of my study is *Safeguarding Employee Privacy in United States - Based Small and Midsized Businesses.*

I am exploring SMB strategies and practices related to employee privacy and would like to interview organizational actors - C suite and midlevel managers of SMBs. The SMB should meet all the following criteria:

1. licensed to operate a business in the Washington DC, Maryland and Virginia (DMV) area.
2. employing between one and 249 personnel
3. have successfully implemented employee privacy strategies.

Interviews with small business participants may provide helpful insight and understanding to increase knowledge and mitigate harms from invasions of employee privacy. I estimate the time commitment for C-suite employees and midlevel managers, to fully participate in the online (phone (call in) option) interviews, will be about 45 minutes. Member checking may be another 30-45 mins. The authorized document collection and delivery to the researcher should be about 1 hour. Upon completion of the study, I will share the research findings with study participants, small business owners, and with fellow university researchers. If you meet the above criteria and are interested in participating in this study, please contact me within 5 days via email. Attached is a consent form further explaining the study. You may express your consent via email by stating “I consent” to participate in a virtual (web-based) audio recorded (phone (call in) is an option) interview. I look forward to hearing from you soon.

Volunteers should ONLY participate if they meet the inclusion criteria for the study.

Sincerely, Encl. (1)

Appendix C: Interview Protocol and Interview Questions

Project: Walden University Doctor of Business Administration (DBA) Study

Type of Interview: Virtual -web – based recorded interview
Date: XX Feb 2022
Place: Online
Online: Interviewer: Kim de Peiza
Interviewee: Consultant __ C-Suite _
Position Title of Interviewee:

Day of Actual Interview:

[Remind the interviewee of the consent form to participate in the study and to audio record the interview (provide copy if required).]
[Turn on the digital audio recorder and test device for functionality.]

[State date and time]. Begin interview:

[Thank the interviewees for their assistance and participation in the interview]. **Stop recording**.

Send an email to inform the interviewee that you will provide him/her a copy of the interpretative transcription file for review, approval, and response.

The following are the interview questions for the two groups of participants:

Privacy Practitioner – Interview Questions for C-Suite Participants:

1. What leadership strategies do you use to effectively safeguard employee privacy?
2. What strategies do you use to handle employee privacy in a remote work design?
3. What leadership strategies do you use to effectively safeguard the privacy of employees when using corporate surveillance tools?
4. What strategies do you use to gain buy-in and resources from your organization to ensure employee privacy is safeguarded?
5. How is the effectiveness of your employee privacy strategies assessed?

6. What supporting organizational processes do you use to determine if your policies and strategies are being effective?

7. What were the key barriers to implementing the employee privacy strategy?

8. How did you address the key barriers to implementing the employee privacy strategy?

9. What other information would you like to share about the strategies you developed and implemented to effectively safeguard employee privacy?

The following are the interview questions I asked specifically to the consultant participants:

Privacy Practitioners – Interview Questions for Consultants:

1. What size of organizations have you supported for employee privacy initiatives?

2. From what sectors are most of your clients?

3. What is the focus of your consulting on employee privacy?

4. What information can you tell me about your consulting experiences with employee privacy?

5. As you are able, please what are two small or midsized company websites with robust employee privacy policies that you can recommend to me?

6. As you are able, please which privacy practitioner can you refer me to from either a small or midsized company that you may have supported, so that their exemplary strategies and perspectives may be included in my study?

Appendix D: Study Participant Thank-You Note

Dear Study Participant,

Thank you for the opportunity of meeting with me and providing honest information, which will significantly impact the results of my doctoral study. I sincerely appreciate the information you have provided and reiterate its confidentiality. As we discussed at the conclusion of our interview, you will receive an email with the transcribed interpretative file within the next **96** hours. It was a pleasure meeting you and learning about your proactive efforts to ensure effective employee privacy strategies.

Sincerely,

Appendix E: Study Participant Interpretative Responses File

Dear Study Participant
As we discussed at the conclusion of your interview, attached is the data interpretation file from the interview session, for the member checking activity. Should you concur with the data interpretation file, no response is necessary. Nonreceipt of a reply within **72 hours** provides concurrence.

Should you disagree with my interpretation of any of your responses, please provide corrections as necessary to me within the next **72 hours** via email. You may expect a revised data interpretation file incorporating your comments within 1 day. Should you concur with the revised data interpretation file, no response is necessary. Nonreceipt of a reply within **72 hours** provides concurrence.

If you have questions, please feel free to contact me via email at
kim.depeiza@waldenu.edu