Middle East Journal of Applied Science & Technology (MEJAST)
Volume 8, Issue 3, Pages 61-81, July-September 2025

Privacy Concerns towards Information Privacy in Hybrid Teams: A Mauritian Context

Rooma Ramasamy[1*], Dr. Vinaye Armoogum[2] & Dr. Perienen Appavoo[3]

[1]*Open University of Mauritius, Moka, Mauritius.* [2]*University of Technology Mauritius, Port Louis, Mauritius.* [3]*Open University of Mauritius, Moka, Mauritius. Corresponding Author (Rooma Ramasamy) Email: rooma.ramasamy@gmail.com*[*]

DOI: https://doi.org/10.46431/MEJAST.2025.8305

Article Received: 15 May 2025 *Article Accepted: 25 July 2025* *Article Published: 28 July 2025*

ABSTRACT

Innovative technology has revolutionized the future of work and will continue to play a vital role in hybrid working arrangements. Technology brings forward the introduction of new threats which increases privacy concerns amongst users. Research around privacy concerns has been explored using different lenses with variance in findings. The Privacy paradox theory has been put forward in various studies as an explanation for inconsistencies where users report having worries about their online privacy but have irresponsible online behavior. This study will examine the privacy paradox theory in the hybrid working environment. A quantitative methodology on a sample population working in hybrid mode (N=204) was followed by using an adaptation of the Concern for Information Privacy scale. The key findings of this study conclude a correlation between behavior and privacy concerns with a p-value of 0.012 but however having a weak relationship. It was also found that there is a disparity of behavior in the working generation with baby boomers showing more concerns and having positive behavior than Gen Z. Gender also influences behavior and concerns, with females exhibiting different behaviors as compared to males. There is a strong positive correlation between privacy awareness and concerns and between privacy awareness and behavior.

Keywords: Privacy Concerns; Privacy Paradox; Hybrid Teams; Concern for Information Privacy Scale; Privacy Attitude; Privacy Behaviour; Working Generation Privacy Behaviour.

1. Introduction

Personal data gathering and its use by organizations has become a source of confusion for people. Information and Communication Technology (ICT) is often associated by having to disclose personal information about the self and may result in several misuses (Cram et al., 2019). News stories concerning privacy are legion, ranging from major incidents like the Equifax and Cambridge Analytica data breaches to minor ones like the priest who came out as gay after Grindr sold location data to users or the people utilizing smart home technologies to track their ex-partners (Gerber's et al., 2023). Our lives are greatly dependent on and enhanced by the continuous revolution of however, there is a detrimental risk to the security of personal information and privacy (Dong, 2024). The introduction of innovative technologies such as generative AI, biometrics, and driverless vehicles will make privacy issues based on technology, which was already significant, far more complex (Kim et al., 2023). In addition, the rising dependence on software and cloud services, respectively, makes privacy maintenance more difficult. Considering data is kept on unstable cloud computers in a virtual environment, improper handling could result in privacy violations (Ahmadi, 2024). Likewise, Nower (2023) iterates the need for privacy defenses with the adoption of microphones and voice assistants in IOT devices. This gives rise to privacy concerns. Previous research has demonstrated that privacy concerns may be associated with an individual's subjective beliefs about fairness regarding privacy. It also relates to the unease and concern that customers have with the collection and usage of their personal data. Privacy concerns are closely linked to how much a user feels that they have no control over their personal data (Jamin et al., 2019).

Due to the worldwide COVID-19 pandemic, remote work or also referred as work from home (WFH) have since proved to be the new way of working. Because of the work-life balance, it is currently the option that many employees choose. The "hybrid" WFH paradigm, which allows for both in-person and remote work, is likely to

gain more momentum with the cost of having significant impact on security concerns. Across all businesses, there are continuous cybersecurity threats and data breach risks since data is handled by the employees in their home computers and mobile devices, where the security measures can be compromised by malicious hackers (Rajkumar et al., 2024). Personal data, which is information about a named or distinguishable individual, is gathered and used practically everywhere and has evolved into the modern era's equivalent of crude oil. The hazards to personal data (for example, person's name, phone number, and location information) unavoidably rise as the value of personal data grows. Also, controlling personal data is also becoming increasingly challenging due to rapid technological advancement and innovation, particularly with data-intensive online activities (Solove, 2015).

Significant studies have explored privacy concerns in various scenarios such as in online social networks, wearable health devices, the internet, cloud computing, banking, governance, e-commerce, financial institutions, and the healthcare sector (Rath & Kumar, 2020) as well as in the age of big data, from a theoretical perspective around privacy theories and even non-privacy theories (Kim et al., 2023). The literature review leaves room for further interpretation with notable gaps. As at date, privacy concerns still need to be investigated across different domains and regions. There is still some disparity in gender research and more granularity is required to explain the disparity in concerns and behavior. Considering the nuanced relationship between these variables, awareness has also not been tested in this context.

Therefore, the purpose of this paper is to understand privacy concerns towards information privacy in a hybrid working environment. The objectives of this paper are to firstly address limitations in the privacy paradox research, not to date explored in the future of work; and secondly in this context explore the concepts of privacy concerns, behavior and awareness while understanding the role of gender and the five generations in the workplace.

This paper is structured by starting with a deep dive into the literature review, presented in section 2, followed by the methodology in section 3. Result analysis and discussion are detailed in section 4, and recommendations and conclusions will be provided in section 5.

1.1. Study Objectives

The objectives of this study are to:

1) Examine the relationship between privacy behavior and concerns.
2) Investigate the influence of age within the working generation on privacy concerns and behaviour.
3) Assess the variation in privacy concerns across different working generations.
4) Evaluate the impact of gender on privacy behaviour and concerns.
5) Analyse the correlation between privacy concerns and awareness.
6) Explore the relationship between awareness and privacy behaviour.

2. Related Works

This section gives an overview of research that has been conducted previously on virtual teams and privacy concerns. The outline of the prior work done gives a sense of the research in question. According to Marshall and

Rossman (2006), the literature review gives visibility over the findings of studies that are closely connected to the one being conducted. It connects a study to a wider, ongoing literary discussion. Bridging the gap and expanding previous research. Therefore, hybrid teams and constructs around privacy concerns will be explored. Theories will also be put forward with emphasis on the privacy paradox being the foundation of this study.

2.1. Virtual and Hybrid Work

One of the most notable transformations in the workplace initiated by the COVID-19 pandemic in 2020 was the rapid transition of a significant segment of the workforce to remote work, also known as teleworking, virtual and/or hybrid work (Grobelny, 2023). Hybrid work represents a flexible employment model accommodating a combination of in-office, remote, and mobile workers. It empowers employees with the freedom to choose their preferred working environment and methods, optimizing productivity. Emphasizing a people-centric approach, hybrid work fosters enhanced productivity and job satisfaction while tackling common remote work challenges like isolation and the absence of a communal atmosphere. This model offers greater adaptability, granting employees the choice to work from home or any conducive location. In the realm of hybrid work, the traditional corporate office is redefined, evolving into a dynamic ecosystem where employees operate from home, shared workspaces, and the office interchangeably based on task requirements (Vidhyaa & Ravichandran, 2022). The authors identify four types of hybrid working models. These are flexible hybrid work model, fixed hybrid work model, office-first hybrid work model and remote-first hybrid work model.

Sostero et al. (2020) have another view, the typical teleworker holds a high-level position, is highly educated, experienced, and well-paid, and regards the autonomy that they are afforded as a privilege correlated with a high professional standing. With very few exceptions, telework, remote work, virtual work and work from home all refer to the same work mode. The broadest definition of remote work is when work is done entirely or in part at a location other than the default location. As a subset of remote work, telework is defined as distant work conducted with the use of digital equipment. Work from home refers to work that is done at home rather than in third places, as is the case with remote work and telework. The new word ‘hybrid work’ became popular during COVID-19 and refers to work that is done in part from the employer's premises and in part from the employee's home or another location. The concept of hybrid work will be applied in this paper.

2.2. The Concept of Privacy

The main source of communication in hybrid work is computer-mediated (Haines et al., 2018), to support teamwork in communicating as indistinctly, seamlessly, and logically as possible, the adoption of advanced communications solutions is essential (Schulza & Krumm, 2017). However, privacy is becoming increasingly important with the use of computers, networks, mobile devices, as well as additional devices for business process automation, communication, and other aspects of daily life. Although the applications make daily living more convenient, various organizations also gather user-specific data that is required to customize the data for convenience. Even in the absence of an individual's agreement, the information collected about them may be used. Two primary information problems have been brought up by this information gathering and storage, namely Security issues and Privacy Issues (Rath & Kumar, 2021).

According to Solove (2015), privacy is “a concept in disarray”. Information privacy is a difficult area of the law considering the rapid changes in technology, especially following the commercial success of the World Wide Web. Because this is discussed in many different social science domains, privacy is referred to as an "umbrella phrase" (Solove, 2015). Although Jan Holvast (2009) believes that privacy issues can be said to be as old as mankind, in 1890, lawyers Warren and Brandeis documented that as old as the principle of common law is, individuals must have the same protection in person and in property and the right to be left alone in their paper ‘The Right to Privacy’. However, despite the importance of privacy as a basic human right, legal protection was absent until the end of the 19th century (Shank, 1986). Individual privacy is characterized by terms like private, quiet, isolated, interruption, intrusion, and absence of disruptions. It could have anything to do with someone's ownership of information and control over the sharing mechanism, either directly or indirectly. Individuals are more concerned about information privacy because of their increased use of new technology and their evolving environment. Resources of worth require protection of their privacy. Individual privacy concerns are therefore a serious problem when it comes to the storing, analyzing, sharing, and preserving of information in ICT (Rath & Kumar, 2021).

2.3. Privacy Concerns

The emergence of the "concern" aspect about information privacy is not surprising, given the variety of information systems and the pervasive (mis)use of information. The lack of control over the protection and use of information is the root cause of privacy concerns. Many theories and measuring tools have been used to operationalize privacy concerns beyond their conceptual definition, such as the Concern for Information Privacy scale (e.g., Dinev & Hart, 2006; Malhotra et al., 2004; Smith et al., 1996). Empirical research has proven the construct's validity (Hong & Thong, 2013) and robustness (Lowry et al., 2011; Zhou, 2011).

Researchers have thoroughly examined users' privacy behaviors considering the seriousness of information risk. A lot of focus has been on an individual's subjective evaluation of the risk to their privacy when it comes to information, which is known as privacy concerns. Previous research has shown that the adoption of ICT services is significantly influenced by concerns about privacy (Dinev & Hart, 2006). However, privacy concerns do not take into consideration the variety of ways that consumers may react to privacy threats. For instance, users tend to underestimate or disregard the risk of repeated data breaches, even if they may raise privacy concerns (Ponemon, 2014). People may become hopeless about internet privacy because of frequent data breaches, believing they have no control over personal information (Kwon & Johnson, 2015).

The potential for harm from the improper access and use of personal data is the basis for privacy concerns. People can simply reduce the risk of information misuse by opting not to disclose personal information whenever they have the option to do so. This is because they want to avoid the possibility that online companies will misuse their information and cause them to suffer a loss (Van Slyke, Shim, Johnson & Jiang, 2006). As a result, people who are overly concerned about their privacy would be less willing to share personal information. Research has shown that privacy concerns significantly influence people's propensity to provide personal information in a variety of online settings (Dinev & Hart, 2006; Taddicken, 2014). Li (2012) identified fourteen theories that relate to privacy concerns, including privacy calculus theory (Dinev & Hart, 2006), protection motivation theory (Rogers, 1975), theory of planned behavior (Ajzen, 1991), and personality theory (Goldberg, 1990). Guided by many theories and

relying on varying degrees of causality and research methods for support, studies have attempted to systematically explain how certain variables (or constructs) are linked to privacy concerns.

Helen Nissenbaum's concept of Contextual Integrity (CI) attempts to address people's inconsistency between their privacy concerns and actual behavior that is data sharing despite stating concerns. Privacy is violated when social settings' established informational norms are broken. CI is composed of both normative and descriptive elements. It determines whether a breach of privacy is justified by evaluating when others are likely to perceive it as such. A breach is considered improper and a privacy issue if the norms support common contextual goals and core ethical principles. But not every breach of the norm is bad if the standard is flawed in the first place (Nissenbaum, 2004). According to Wirth (2017), the definition of privacy in essence conveys a socio-psychological perspective leading to privacy-related behaviors.

Kokolakis (2017) thinks that a few scholars have drawn a comparison between privacy behavior and privacy concerns. Earlier studies have found a significant influence of privacy attitude on privacy behavior. Despite their close relationship, privacy attitudes and privacy concerns are two quite different phenomena. While privacy attitudes relate to the evaluation of particular privacy actions, privacy concerns can be very general and, for the most part, are not restricted to any particular situation.

2.3.1. Privacy Behavior

Berendt et al. (2005) examined user's privacy preferences during online shopping against their behavior and found a significant difference. The defining factors involved were:

Perceived benefits: If users believe they are getting something in return, such as a discount or a tailored shopping experience, they can be more inclined to divulge personal information.

The perceived risks: If users feel that their privacy is in jeopardy, they might be less inclined to divulge sensitive information.

Perceived ease of use: If providing personal information is simple, users might be more likely to do so. The perceived value of privacy: If users don't think privacy is important, they can be more ready to divulge personal information.

2.3.2. Privacy Awareness

Despite privacy awareness having well-recognized benefits, its definition is still unclear. According to some academics, privacy awareness is the awareness of the risks and repercussions that could arise from disclosing personal information. Other academics refer to privacy awareness as being users' awareness of the privacy policies of the services they utilize or the regulations that protect them (Soumelidou & Tsohu, 2021).

However, despite regulatory efforts (for example, the Data Protection Act in Mauritius, and GDPR in the European Union), previous research indicates individuals have no awareness of protecting their privacy and personal information. An increase in cybercrimes has been noted around the COVID-19 period, impacting both the public and private sectors, with user awareness being one of the root causes (Raghad et al., 2021).

2.4. Privacy Paradox and Privacy Calculus Theory

Gerber et al. (2018) believe the contrast between privacy attitudes and behaviors, also referred to as the privacy paradox, has been the subject of multiple attempts by privacy scholars to find a rationale. User's attitude towards several privacy decision behaviors is indicated by their privacy concern. Privacy research evolves around this theme. Scholars have thoroughly studied the favorable influence link between privacy concerns and privacy behaviors such as Xu et al. (2010) found that mobile social media users tended to stop using social media if they thought their personal information had been misused or obtained through unidentified means.

However, no thorough explanation for the privacy paradox has been discovered to date, even though there are several theoretical reasons for the privacy paradox as well as empirical study findings about the relationship of individual elements on privacy behavior and attitude. Privacy is valued by everyone, unfortunately, nowadays people strongly feel their privacy is no longer within their control and they are helpless to take any action regarding it (Cronk, 2022). People voluntarily, and sometimes unknowingly contribute data to Internet-based applications, and that may expose them to privacy risks, violations, and harms (Kitkowska et al., 2018).

On the other hand, the privacy calculus theory is the rational analysis of an individual when they bargain with the disclosure of their personal data against perceived benefits (Plangger & Montecchi, 2020). This theory asserts that users do not consider technology-associated risks but instead the perceived benefits. The perceived benefits are a motivator whereas the risk sacrificed is perceived to be lower (Bhatia & Breaux, 2018). However, their willingness to use these technologies is unaffected by these risks. According to research, individuals accept new technology more often for convenience than for privacy concerns (Gashami et al., 2016).

Structural and psychological reasons have been identified as to why individuals cannot protect their privacy. Individuals are not well equipped for rational decision-making regarding privacy. Often, organizations do not use layman's terms to communicate how the individual’s information is handled, such as legal information. In turn, becomes a cascading effect where people are not well-equipped to make logical choices about privacy. They may be unaware of the activities that impact their privacy, also referred to as asymmetric information. Most of the time they will not take the time to read and understand fully disclosed information. Even with awareness and understanding, it is most of the time difficult to find alternatives or asymmetric power unless technology is sacrificed (Cronk, 2022). Solove (2015) has observed that the approach of "privacy self-management" through notice and choice mechanisms places the responsibility on individuals to safeguard their privacy.

However, the extensive use and ubiquity of digital technology have rendered true control over personal information unattainable. The sheer volume of choices overwhelms individuals, leading to a deficient accountability system that shifts risks onto individuals who are essentially left with no viable option other than agreeing by clicking the "I Agree" button. Concisely, the privacy calculus concept states that a user is expected to voluntarily give up their data if the advantages of sharing it are projected to outweigh the drawbacks. The observed disparity between the expressed concerns or attitudes and the actual behavior results from the fact that users can still voice concerns about the loss of their data (Gerber et al., 2018). Kitkowska et al. (2018) in a study, using Solove’s framework, identified seven dimensions of privacy concerns: insecurity, exposure, unauthorized access, secondary use of data, misuse of

data, distortion and interrogation. Improper access and secondary use of data correlate with two of the four dimensions identified by CFIP. Kitkowska et al. (2018) further discuss that high concerns about security are expressed, people want information regarding data security breaches and generally expect to be guaranteed safety online. The findings of the study also indicate a worry about exposure, which is online presence and information visibility. They also want control of their personal information and don't want this to be used without their permission or knowledge. Of importance is also concern about the secondary use of data for example sharing or selling with external parties or misuse such as malicious use of information or blackmail. On the other hand, Buchanan et al. (2007) maintain that awareness of issues such as improper access, unauthorized data collection, and unauthorized secondary use amongst others may alter behavior.

2.5. Challenges of privacy concerns in a nutshell

Key related studies have been analyzed to build the foundation of this research. A summary is provided in Table 1.

Table 1. Summary of related studies (Dimodugno et al., 2021)

Author	Paper Title	Research Focus	Challenges & Gaps	Clarity	Novelty
Dimodugno et al. (2021)	The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach.	Examine the relationship among the variables of perceived privacy concerns, perceived privacy risk, perceived privacy control, and trust.	Privacy issues are experienced by professional workers when sharing personal information. Study not applicable to different domains and regions.	Variables put forward were correlated providing clarity to the research objectives.	Using the game theory to analyse actions, strategies and payoffs.
Gerber et al. (2018)	Explaining the privacy paradox: A systematic review of the literature investigating privacy attitude and behavior.	Privacy paradox explanations and identifying the factors those are most relevant for the prediction of privacy attitude and behavior.	Gender was found to weakly predict privacy behavior.	Challenge remains to draw overall conclusions	In-depth review of attitude vs behavior - Evolving privacy paradox with new technologies - Global Diversity.
Rath & Kumar (2020)	Information privacy concern at the individual, group, organization and societal level - a literature review.	Privacy concerns on systems in the various domains (E-Governance, E-Commerce, E-Health, E-Banking and E-Finance), and at different levels, i.e.	More research is needed to understand behavior vs stated concerns. More variables to understand factors influencing actual privacy behavior.	Clarity on different domains.	Novelty lies in addressing privacy concerns at the individual, group, organizational and societal levels.

		individual, group, organizational and societal.	More granularity is needed to distinguish concerns.		
Kim et al. (2023)	Privacy concern and its consequences: A meta-analysis.	Relationship between privacy concern and its consequences such as trust, protection behavior.	Nuanced relationship between variables which require further analysis.	Broad evidence but however consistent with the relationship between privacy concerns.	Two decades of research has been analysed.
Jamin et al. (2019)	Privacy Concerns of Personal Information in the ICT usage, internet and social media perspective.	Exposure of personal data by users in ICT usage.	Awareness of privacy concerns towards personal information when accessing the internet.	The limitation of the paper does not test assumption s made that is the variables of awareness and privacy concerns.	In general ICT, the Internet and social networking affect the privacy concerns of personal information.
Soumelidou & Tsohou (2021)	Privacy Awareness and Its Impact on the Use of Online Services: A Study on Greek Users.	Privacy Awareness among Greek users.	Privacy awareness varied significantly. Key factors influencing awareness are digital literacy, education and socioeconomic factors, age and experience, and cultural factors. Despite higher awareness users continued to share personal information due to convenience. Trust variable was also put forward.	This paper provided key implication s on the relationship between awareness and behavior.	Localised research taking into account the cultural and socioeconomic factor.
Malhotra et al. (2004)	Internet privacy concerns and their antecedents: A model and research	Explore concerns on collection and use of personal	Since this study was conducted in 2004, technology has	The study provides clarity on the causes	This paper at the time provided insights into the emerging topic

	propositions.	data by online business. Identifies causes of privacy concerns.	changed leaving room for more privacy risks and concerns.	of privacy concerns.	of privacy concerns.
Sorum et al. (2022)	A Gender Perspective on GDPR and Information Privacy.	Gender differences in privacy behavior.	Limited population.	Focused research on gender differences.	Applying the gender perspective from a GDPR lens.

In summary, the literature review provided an in-depth comprehension of the key themes and debates surrounding privacy concerns used as a basis for this paper. Novelty topics were analyzed. Notably, the effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information was analyzed using the game theory, a model used to analyze situations and how subjects called players make interdependent decisions. The review also produced from another perspective, privacy paradox in terms of innovative technologies with the identification of factors relevant for the prediction of privacy attitude and behavior. Global diversity was a novel theme put forward in the discussions. Furthermore, privacy concerns at the individual, group, organizational and societal levels was reviewed in different domains. Privacy concerns in the lens of the cultural and macroeconomic factor was studied. Another original study deep dived the gender perspective. In general ICT, the Internet and social networking and how these affect the privacy concerns of personal information was reviewed.

While considerable progress has been made around privacy concerns, there remains significant gaps, challenges and inconsistencies. There is still a challenge today to understand privacy concerns in different settings, domains, and countries. Adding to that, it is still difficult to ascertain the position of gender differences. While awareness is a key variable today there still is room for more clarity on its effects. There is also a variation of findings between the variables privacy concerns, awareness and behavior which needs to be further explored. With the lack of consensus on the future of work and evolving privacy issues, there is an opportunity for future research to address these ambiguities. Therefore, to contribute to the work already accomplished, this research has an objective to explore the concepts of privacy concerns, behavior and awareness while understanding the role of gender and the five generations in the workplace, in a hybrid work environment where further exploration is required.

This literature review sets the foundation for the present study, which aims to fill the identified gaps by analyzing the concepts of privacy concern, behavior, and awareness to better understand the privacy paradox in hybrid work. By building on the existing body of knowledge, this research will contribute to a deeper understanding of privacy concerns and provide implications for both theory and practice.

3. Methodology

According to Durbarry et al. (2018), every researcher has a different lens in viewing the research domain, therefore how studies are conducted, will vary. This section emphasizes the methodology guiding this research.

This study examines how the dependent variables privacy concerns, behavior, and awareness relate to the independent variables age and gender for professionals working in a hybrid environment. Additionally, the study also aims to analyze the influence of behavior and awareness on privacy concerns.

The research design used in the study is quantitative. The purpose of quantitative approaches is to examine events and their interactions in a methodical manner by working with numbers and anything measurable. This approach provides answers to the issues of how quantifiable variables relate to one another in order to describe, forecast, and regulate a phenomenon (Cresswell, 2009).

The evolutionary Concern for Information Privacy (CFIP) scale was developed by Smith, Milberg, & Burke (1996) enabling the identification and measurement of the main dimensions of individual privacy concerns regarding organizational information privacy practices. Buchanan et al. (2007) developed using the CFIP as a foundation and validated a scale to measure online privacy concerns and protection for use on the internet. The questionnaire for this study was adapted to this scale. Section A contains questions related to demographics, Section B behavior behavior-related questions, Section C is privacy concern-related questions and Section D is on Awareness. The questions were presented on a five-point Likert scale (1 = disagree; 5 = agree).

Cresswell (2009) emphasizes the importance of ethics throughout the whole research process. As such, participants have been informed about the purpose of the study, how the data will be used, handling and storage of information collected. Personal data has not been collected. Participants could also withdraw the questionnaire should they not feel comfortable in providing their input.

3.1. Sample

The target population is individuals in the ICT industry known to be working in a virtual setting in Mauritius. Recruitment was done via LinkedIn, and emails were sent to organizations members of the Outsourcing & Telecommunications Association of Mauritius (OTAM). The questionnaire has a preliminary section about the type of work setting, that is face-to-face, or hybrid allowing capturing a sample of 218 respondents working in a hybrid mode. However, after eliminating incomplete responses, 211 responses were used as a basis. A combination of purposive and snowball sampling approach was adopted considering the complexity of identifying the population which was previously unknown. Prior to sharing the questionnaires with the sample population, a pilot study was conducted with selected respondents working in a virtual setting resulting in a few minor rewordings for clarity and changes to the structure of the questionnaire for efficiency. From an ethical perspective, a statement has been built into the questionnaires on Google Forms to stipulate the purpose of the study and emphasise that personal data will not be collected. Participants are also informed that they can withdraw from the survey at any moment, and they also have the freedom to omit any information they deem embarrassing. The methods used was strictly aligned to the research objectives and approved by the ethics committee of the Open University of Mauritius after being carefully weighed against potential harm.

3.2. Hypothesis proposal

Previous studies have tried to put forward the privacy paradox theory to explain for disparities between privacy concerns and actual behavior. However, findings have left room for further investigation and interpretation. Therefore:

A hypothesis has been developed to suggest that behavior and privacy concerns do not have a relationship. It implies that there is a nonexistent relationship between these two dependent variables.

H01: There is no significant relationship between behavior and privacy concerns;

This hypothesis proposes the independent variable of age in the working generation has no significant relationship with the dependent variables' privacy concerns and behavior.

H02: There is no significant relationship in the working generation with privacy concerns and behavior;

To understand the relationships of the variables further, the following hypothesis puts forward that there is no inconsistency in privacy concerns among the four working generations.

H03: There is no significant disparity of behavior between the different working generations;

The below null hypothesis puts forward that gender does not influence privacy behavior and concerns.

H04: Privacy behavior and concerns are not determined by Gender;

Awareness in this hypothesis does not have any effect on privacy concerns meaning there is no influence between these two dependent variables.

H05: Privacy concerns have no significant correlation with awareness;

Awareness in this hypothesis does not have any effect on behavior meaning there is no influence between these two dependent variables.

H06: There is no significant relationship between behavior and awareness.

Taking into account the key variables determined in this study, the below model is proposed as the driver of this research in Figure 1:

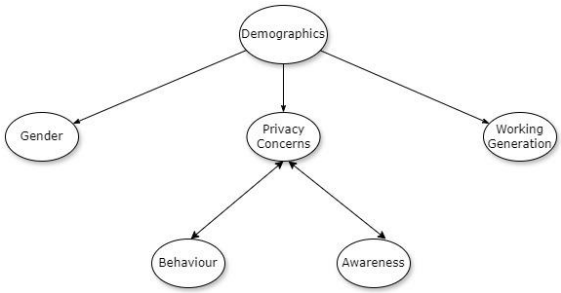


Figure 1. Proposed Model

The literature review therefore produced an overview of key concepts which may be used as a basis to understand privacy concerns in hybrid teams.

3.3. Methods of Analysis

Cresswell (2009) recommends that quantitative studies first use descriptive statistics to analyse the demographics of the participants before then conducting hypothesis testing. Following this approach, descriptive statistics depicted the characteristics of the respondents in terms of gender and age, a key variable to determine working generation behavior, concern, and awareness in this study.

Pearson correlation was run to assess the strength and direction of the relationship between the variables concern, awareness, and behavior. A multivariate test in the form of Multivariate Analysis of Variance (MANOVA) was

conducted to understand statistical differences between the two dependent variables of concern and behavior across the different levels of the working generation, that is the independent variable age. MANOVA was also the appropriate test to understand the role of gender in privacy behavior and concerns. Spearman Rho test was conducted to investigate the disparity between the different working generations.

4. Results, Analysis and Discussion

This section will detail the result and analysis of the findings and therefore be a basis for discussion.

Once the survey was closed, the data was exported into Microsoft Excel format for the first high-level processing. Post some minor structuring and removal of incomplete data, it was uploaded on the statistical software IBM SPSS where the data was further grouped, outliers checked, and variables renamed for ease of analysis.

4.1. Normality

A test of normality was performed on the dependent variables to validate whether the data collected followed a normal distribution. P value was above 0.5 as shown in figure 2, the data is consistent with a normal distribution and therefore indicating normality in variables Age and Gender.

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Age	.329	218	.000	.811	218	.000
Gender	.394	217	.000	.621	217	.000

a. Lilliefors Significance Correction

Figure 2. Test of normality

4.2. Validity and Reliability

Content and face validity were conducted to ensure the questionnaire covered what it intended to measure as well as have a good level of comprehension and understanding. Improvements and suggestions were carefully taken into consideration and implemented where applicable.

In regards to reliability, a Cronbach Alpha test was run to ensure consistency of the adapted scale used. The result obtained, as shown in figure 3, is an alpha of 0.8 therefore indicating a good level of reliability. Should the questionnaire be administered to another sample population, the result will be the approximately the same.

Case Processing Summary

		N	%
Cases	Valid	196	89.9
	Excluded[a]	22	10.1
	Total	218	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

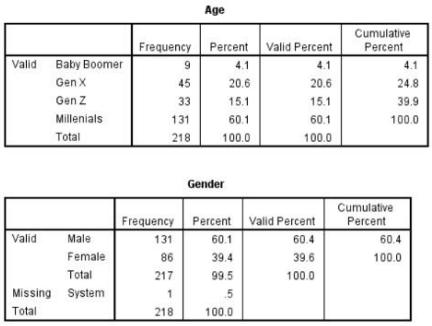
Cronbach's Alpha	N of Items
.843	4

Figure 3. Cronbach Alpha test

4.3. Respondents analysis

Demographics were also part of the questionnaire to understand the role of gender and age. A total of 204 complete responses have been received, excluded was incomplete information. The percentage of respondents male is 63.7%

and female 37.3%, within the working generation, comprising of Baby Boomers (Born 1946 - 1964) which was 4.1% of respondents, Generation X (Born 1965 - 1980) 20.6% of respondents, Millennials (Born 1981 - 1996) 60.1% of respondents and Generation Z (Born 1997 - 2012) 15.1% of respondents. This can be seen in figure 4:



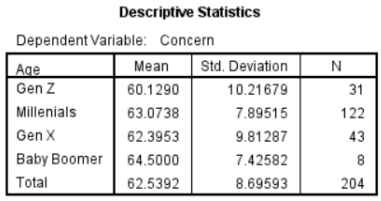
Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Baby Boomer	9	4.1	4.1	4.1
	Gen X	45	20.6	20.6	24.8
	Gen Z	33	15.1	15.1	39.9
	Millenials	131	60.1	60.1	100.0
	Total	218	100.0	100.0	

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	131	60.1	60.4	60.4
	Female	86	39.4	39.6	100.0
	Total	217	99.5	100.0	
Missing	System	1	.5		
Total		218	100.0		

Figure 4. Demographic analysis of respondents



Descriptive Statistics

Dependent Variable: Concern

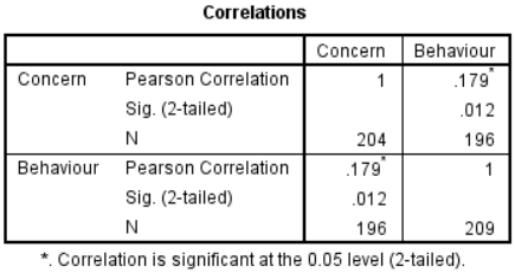
Age	Mean	Std. Deviation	N
Gen Z	60.1290	10.21679	31
Millenials	63.0738	7.89515	122
Gen X	62.3953	9.81287	43
Baby Boomer	64.5000	7.42582	8
Total	62.5392	8.69593	204

Figure 5. Descriptive analysis of respondents and privacy concerns

Baby Boomers and Millennials seem to be the most concerned on average, while Gen Z shows slightly lower concern. However, the Baby Boomer group has a very small sample size (N = 8), which may limit the generalizability of its results. Gen Z shows more variability in concern scores, which could suggest differing levels of concern within that generation.

4.4. Hypothesis

H01: There is no significant relationship between behavior and privacy concerns.



Correlations

		Concern	Behaviour
Concern	Pearson Correlation	1	.179*
	Sig. (2-tailed)		.012
	N	204	196
Behaviour	Pearson Correlation	.179*	1
	Sig. (2-tailed)	.012	
	N	196	209

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 6. Correlation Concern/Behavior

As detailed in figure 6, the p-value of 0.012 shows the correlation is statistically significant at 0.05 level, however the relationship between the two variables of concern and behavior is weak. There is a slight tendency for respondents reporting a higher level of concern to also exhibit corresponding behavior increases. However, the correlation being at 0.05 is low, meaning the relationship is not strong. The null hypothesis can be rejected in this case as there is a statistically significant correlation between behavior and privacy concerns but with a weak relationship. In terms of practical considerations, the privacy paradox theory in this context can explain this disparity, where according to Solove (2015), respondents ascertain their concerns over privacy-related topics but

with a discrepancy in their behavior. Hoffmann et al. (2016) found that individuals may disregard risk cues or behavioral recommendations because they believe that adopting stricter privacy practices is useless. Previous studies have mixed results in trying to understand the discrepancy between privacy concerns and behavior where this mismatch is explained by the privacy paradox (Wisniewski & Page, 2022).

It is key, however, to understand the relationship between the strength of the two variables, therefore a subgroup analysis has been done. The relationship between behavior and concern might be stronger in one category (working generation, gender) than in another. The hypothesis is therefore:

H02: There is no significant relationship in the working generation with privacy concerns and behavior.

Baby Boomers report the highest average concern, followed closely by Millennials and Gen X Gen Z has the lowest average concern. The standard deviations as shown in figure 7, indicate the spread of concern scores within each group, with Gen Z showing the most variability in concern scores. This implies differences in concern levels across generations, with older generations (Millennials, Gen X, Baby Boomers) showing higher concern levels compared to Gen Z. The null hypothesis can therefore be rejected. Soumelidou and Tsohou (2021) also found in their study conducted in Greece, that older users showed higher concern for privacy. Gerber et al. (2018) from a systematic review could deduct how age groups have different levels of privacy concerns where this has a role in the privacy paradox theory. Millennials and Gen Z tend to sacrifice privacy due to better digital literacy while the older generations are more cautious.

Descriptive Statistics

	Age	Mean	Std. Deviation	N
Behaviour	Gen Z	31.3333	8.98786	30
	Millenials	31.4103	7.80158	117
	Gen X	34.7381	9.46640	42
	Baby Boomer	40.4286	6.26783	7
	Total	32.4337	8.51609	196
Concern	Gen Z	59.8667	10.28468	30
	Millenials	63.1624	7.80358	117
	Gen X	62.6190	9.82022	42
	Baby Boomer	63.8571	7.77664	7
	Total	62.5663	8.68838	196

Multivariate Tests[a]

Effect		Value	F	Hypothesis df	Error df	Sig.
Intercept	Pillai's Trace	.960	2293.936[b]	2.000	191.000	.000
	Wilks' Lambda	.040	2293.936[b]	2.000	191.000	.000
	Hotelling's Trace	24.020	2293.936[b]	2.000	191.000	.000
	Roy's Largest Root	24.020	2293.936[b]	2.000	191.000	.000
Age	Pillai's Trace	.077	2.571	6.000	384.000	.019
	Wilks' Lambda	.924	2.572[b]	6.000	382.000	.019
	Hotelling's Trace	.081	2.574	6.000	380.000	.019
	Roy's Largest Root	.063	4.015[c]	3.000	192.000	.008

a. Design: Intercept + Age
b. Exact statistic
c. The statistic is an upper bound on F that yields a lower bound on the significance level.

Figure 7. Multivariate tests between age, behavior and concerns

Since the MANOVA is significant, additional follow-up analyses for each dependent variable to explore where the differences lie among age groups were done.

H03: There is no significant disparity of behavior between the different working generations.

Descriptive Statistics

Dependent Variable: Behaviour

Age	Mean	Std. Deviation	N
Gen Z	31.0313	8.88451	32
Millenials	31.6560	7.82995	125
Gen X	34.4773	9.32486	44
Baby Boomer	37.6250	9.82617	8
Total	32.3828	8.49247	209

Correlations

			Privacy Behaviour	Age
Spearman's rho	Privacy Behaviour	Correlation Coefficient	1.000	.173*
		Sig. (2-tailed)	.	.012
		N	210	210
	Age	Correlation Coefficient	.173*	1.000
		Sig. (2-tailed)	.012	.
		N	210	218

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 8. Behavior in different working generations

The mean values as shown in figure 8, depict a slight increase in behavior scores as age increases, with Baby Boomers having the highest mean, followed by Gen X, Millennials, and Gen Z. However, the variability is relatively consistent across groups, with Baby Boomers showing the most variation relative to the sample size. The P-value of 0.058 is just above the standard significance threshold of 0.05, which suggests that the generational

differences in Behavior are not statistically significant at the 0.05 level. The null hypothesis can be accepted, however, with a larger sample there is a possibility to investigate further, considering Baby Boomers was a relatively smaller sample.

H04: Privacy behavior and concerns are not determined by Gender.

Previous studies have explored the effect of gender. The significance level of .044 in figure 8 indicates that there is a statistically significant difference in the dependent variables based on gender. Therefore, the evidence of a statistically significant difference in privacy behaviors between the two genders is present. Within the context of this study, gender may influence privacy behavior and concerns, with females potentially exhibiting different privacy behaviors as compared to males. The significant F-value for gender means gender influences the dependent variables collectively. This implies that male and female participants may respond differently across the measured behaviors. Sorum et al. (2022) conducted a study in Norway to investigate gender differences and found increased privacy concerns in women where they expressed higher levels of concern about privacy issues compared to men. This included apprehensions regarding data sharing, surveillance, and personal information security. Gerber et al. (2023) found females have more privacy-protecting behaviors than men, as they are more cautious.

Multivariate Tests[a]

Effect		Value	F	Hypothesis df	Error df	Sig.
Intercept	Pillai's Trace	.983	5454.854[b]	2.000	193.000	.000
	Wilks' Lambda	.017	5454.854[b]	2.000	193.000	.000
	Hotelling's Trace	56.527	5454.854[b]	2.000	193.000	.000
	Roy's Largest Root	56.527	5454.854[b]	2.000	193.000	.000
Gender	Pillai's Trace	.032	3.182[b]	2.000	193.000	.044
	Wilks' Lambda	.968	3.182[b]	2.000	193.000	.044
	Hotelling's Trace	.033	3.182[b]	2.000	193.000	.044
	Roy's Largest Root	.033	3.182[b]	2.000	193.000	.044

a. Design: Intercept + Gender
b. Exact statistic

Figure 9. Multivariate Test

H05: Privacy concerns have no significant correlation with awareness.

The Pearson correlation coefficient is 0.538 as shown in figure 10. This indicates a moderate to strong positive correlation between the two variables of concerns and awareness. As one variable increases, the other variable tends to increase as well. Therefore, individuals who express higher levels of awareness also tend to have higher levels of concerns. The null hypothesis is therefore rejected. In other words, the more awareness respondents have of privacy issues, such as risks associated with data collection and misuse, the more likely they are to express privacy concerns. As an example, knowing about the risks of data breaches or how companies share personal data with third parties can lead to heightened concerns about privacy. This relationship can be seen in how people react to increasing media coverage about data privacy issues, such as the Facebook-Cambridge Analytica scandal or the implementation of the General Data Protection Regulation (GDPR). Some seminal studies such as Westin (2003), Smith et al. (1996), and Malhotra et al. (2004) confirm the positive relationship between awareness and concern.

Correlations

		Concern	Awareness
Concern	Pearson Correlation	1	.538**
	Sig. (2-tailed)		.000
	N	204	200
Awareness	Pearson Correlation	.538**	1
	Sig. (2-tailed)	.000	
	N	200	211

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 10. Correlation between concern and awareness

H06: There is no significant relationship between behavior and awareness.

The Pearson correlation coefficient is 0.784 as shown in figure 11. This indicates a strong positive correlation between the two variables of behavior and awareness, suggesting that as awareness increases, behavior tends to improve or increase as well. Soumelidou and Tsoho (2021) in their study conducted in Greece, share similar findings where higher awareness is associated with positive behaviour.

Correlations

		Awareness	Behaviour
Awareness	Pearson Correlation	1	.784**
	Sig. (2-tailed)		.000
	N	211	206
Behaviour	Pearson Correlation	.784**	1
	Sig. (2-tailed)	.000	
	N	206	209

**. Correlation is significant at the 0.01 level (2-tailed).

Figure 11. Correlation between awareness and behavior

5. Recommendations, Conclusion and Future Direction

This section presents the major findings of this study, conclusions, and recommendations as well as future research that can be made to further understand the privacy phenomena which will keep on evolving. Based on the finding on the relationship between behavior and privacy concerns, it was found that correlation between behavior and privacy concerns is statistically significant, but with a weak link. This indicates that respondents have concerns over privacy-related topics but however have behaviors which may compromise their privacy.

A statistically significant difference was found between the two genders in their privacy behaviors. Programs towards privacy education should also have initiatives acknowledging gender based privacy violations. This privacy literacy should be developed taking into account unique challenges and experiences and empower each gender to have the necessary knowledge and tools. Governmental institution must also take a step during policy development to recognize gender based privacy issues and put forward measures with a gender responsive approach. It was also found in this study differences in privacy concern levels across generations, with older generations (Millennials, Gen X, Baby Boomers) showing higher concern levels compared to Gen Z. It is proposed to have Privacy-related laws made available and communicated in simple layman's terms, understandable across all generations, as empowering users will have an increased awareness and therefore make better decisions. Social media can be leveraged for campaigns considering these platforms are popular among Gen Z. Emphasis should be put on how users can protect their privacy and keep their data secure. While demographics can be a factor of influence, it is important to take into consideration implications of cultural, gender-based violence, specific vulnerabilities across generations, therefore introducing additional variables may provide additional insights into this phenomenon in terms of further research.

Additional findings were respondents having more awareness contributed to positive behavior. The more concern they have contribute to better privacy-related choices.

In terms of future directions, it is proposed to:

1) Test privacy concerns and behavior in different environments to assess contextual variations in user responses.

2) Consider respondents' areas of expertise to understand how domain knowledge influences privacy perceptions.

3) Conduct longitudinal studies to compare user insights before and after reading disclaimers and clicking "Agree."

4) Record user feedback both with and without exposure to disclaimers to evaluate the impact of informed consent.

5) Establish independent privacy governance with clear reporting and accountability mechanisms across organizations.

6) Normalize independent privacy audits to build user trust and provide assurance about data handling practices.

7) Embed privacy into end-to-end business processes, including Software development using privacy-by-design, accessible privacy settings, clear policies and employee training ensure transparency in the user data lifecycle, from collection to deletion, to empower informed user choices, promote privacy education at the societal level so all generations understand how to protect their personal data.

Declarations

Source of Funding

This study received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The authors declare that they have no competing interests related to this work.

Consent for publication

The authors declare that they consented to the publication of this study.

Authors' contributions

All the authors made an equal contribution in the Conception and design of the work, Data collection, Drafting the article, and Critical revision of the article. All the authors have read and approved the final copy of the manuscript.

Availability of data and materials

Authors are willing to share data and material on request.

Ethical Approval

This study was approved by the ethics committee of the Open University of Mauritius.

Institutional Review Board Statement

Not applicable for this study.

Informed Consent

All participants in this study voluntarily gave their informed consent prior to their involvement in the research.

References

Ahmadi, S. (2024). Systematic literature review on cloud computing security: Threats and mitigation strategies. Journal of Information Security, 15(2): 148–167. https://doi.org/10.4236/jis.2024.152010.

Ahmed, Y.M., & Al Kahlout, M.I. (2024). A novel model for protecting the privacy of digital images in cloud using permutated fragmentation and encryption algorithms. International Journal of Computer Network and Information Security, 16(5): 35–45. https://doi.org/10.5815/ijcnis.2024.05.04.

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2): 179–211. https://doi.org/10.1016/0749-5978(91)90020-t.

Bhatia, J., & Breaux, T. (2018). Semantic Incompleteness in Privacy Policy Goals. IEEE 26th International Requirements Engineering Conference (RE), Banff, AB, Canada, Pages 159–169. https://doi.org/10.1109/re.2018.00025.

Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in e-commerce: Stated preferences vs. actual behavior. Communications of the ACM, 48(4): 101–106. https://doi.org/10.1145/1053291.1053295.

Buchanan, T., Paine, C., Joinson, A., & Reips, U. (2006). Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology, 58(2): 157–165. https://doi.org/10.1002/asi.20459.

Cram, W.A., D'Arcy, J., & Proudfoot, J.G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43(2). https://doi.org/10.25300/misq/2019/1511.

Cresswell, J. (2009). Qualitative, quantitative, and mixed methods approaches (3rd Eds.). Sage.

Cronk, R.J. (2022). Strategic Privacy by Design, Second Edition. International Association of Privacy Professionals (IAPP). Available at: https://iapp.org/resources/article/strategic-privacy-by-design/.

Dimodugno, M., Hallman, S., Plaisent, M., & Bernard, P. (2021). The effect of privacy concerns, risk, control, and trust on individuals' decisions to share personal information: A game theory-based approach. Journal of Physics: Conference Series. https://doi.org/10.1088/1742-6596/2090/1/012017.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. Information Systems Research, 17(1). https://doi.org/10.1287/isre.1060.0080.

Dong, Z. (2024). System-justifying belief alleviates online privacy concerns: The mediating role of relatedness satisfaction and general trust. Computers in Human Behavior, 154. https://doi.org/10.1016/j.chb.2024.108140.

Durbarry, R. (2018). Research Methods for Tourism Students.

Gashami, J.P.G., Chang, Y., Rho, J.J., & Park, M.C. (2015). Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. Information Development, 32(4): 837–852. https://doi.org/10.1177/0266666915571428.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of the literature investigating privacy attitude and behavior. Computers & Security, 77: 226–261. https://doi.org/10.1016/j.cose.2018.04.002.

Goldberg, L.R. (1990). An alternative "description of personality": The Big-Five factor structure. Journal of Personality and Social Psychology, 59(6): 1216–1229. https://doi.org/10.1037/0022-3514.59.6.1216.

Grey, S. (2023). The future of work: Adapting to remote and hybrid work models in a digital age. Journal of Business & Financial Affairs, 12(1): 443.

Grobelny, J. (2023). Factors driving the workplace well-being of individuals from co-located, hybrid, and virtual teams: The role of team type as an environmental factor in the job demand–resources model. International Journal of Environmental Research and Public Health, 20: 3685. https://doi.org/10.3390/ijerph20043685.

Haines, A., Perkins, E., Evans, E., & McCabe, R. (2018). Multidisciplinary team functioning and decision making within forensic mental health. Mental Health Review Journal, 23(3): 185–196. https://doi.org/10.1108/mhrj-01-2018-0001.

Hoffmann, C.P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. Journal of Psychosocial Research on Cyberspace, 10(7). https://doi.org/10.2139/ssrn.3319830.

Holvast, J. (2009). The future of identity in the information society. Privacy and identity. IFIP Advances in Information and Communication Technology, 298. https://doi.org/10.1007/978-3-642-03315-5_2.

Hong, W., & Thong, J. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. MIS Quarterly, 31(1): 275–298. https://www.jstor.org/stable/43825946.

Jamin, J., Md Arifin, N., Mokhtar, S., Rosli, N., & Mohd Shukry, A. (2019). Privacy concern of personal information in the ICT usage, internet and social media perspective. Malaysian E-Commerce Journal, 3: 15–17. https://doi.org/10.26480/mecj.02.2019.15.17.

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 pandemic. International Journal of Information Engineering and Electronic Business, 13: 1–10. https://doi.org/10.5815/ijieeb.2021.02.01.

Kim, Y., Kim, S.H., Peterson, R.A., & Choi, J. (2023). Privacy concern and its consequences: A meta-analysis. Technological Forecasting and Social Change, 196: 122789. https://doi.org/10.1016/j.techfore.2023.122789.

Kitkowska, M. (2018). User-centric privacy: A study of awareness and attitudes. Presented at the Networked Privacy Workshop, 2018. Available at: https://networkedprivacy2018.wordpress.com/wp-content/uploads/2018/04/kitkowska.pdf.

Kleindienst, D., Nüske, N., Rau, D., & Schmied, F. (2017). Beyond mere compliance, Delighting customers by implementing data privacy measures. In Leimeister & Brenner (Eds.), Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017), Pages 807–821, St. Gallen, Switzerland.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. Computers & Security, 64: 122–134. https://doi.org/10.1016/j.cose.2015.07.002.

Kwon, J., & Johnson, M.E. (2015). Protecting patient data – The economic perspective of healthcare security. IEEE Security & Privacy, 13(5): 90–95. https://doi.org/10.1109/msp.2015.113.

Langheinrich, M. (2001). Privacy by design – Principles of privacy-aware ubiquitous systems. In Abowd, Brumitt, & Shafer (Eds.), Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001), Pages 273–291, Springer. https://doi.org/10.1007/3-540-45427-6_23.

Lowry, P.B., Cao, J., & Everard, A. (2011). Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. Journal of Management Information Systems, 27(4): 163–200. https://doi.org/10.2753/mis0742-1222270406.

Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research, 15(4): 336–355. https://doi.org/10.1287/isre.1040.0032.

Marshall, C., & Rossman. (2021). Designing qualitative research. Sage.

Nissenbaum, H. (2004). Privacy as contextual integrity. Washington Law Review, 79(1): 119–158.

Nower, N. (2023). Supporting audio privacy-aware services in emerging IoT environments. International Journal of Wireless and Microwave Technologies, 11(3): 22–29. https://doi.org/10.5815/ijwmt.2021.03.04.

Ponemon Institute (2014). A year of mega breaches. Ponemon Institute. Available at: https://www.ponemon.org/research/ponemon-library/security/2014-a-year-of-mega-breaches.html (Accessed: 10 August 2023).

Plangger, K., & Montecchi, M. (2022). Thinking beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. Journal of Interactive Marketing, 50(1): 32-44. https://doi.org/10.1016/j.intmar.2019.10.004.

Raghad, K., et al. (2021). Cybercrimes during COVID-19 Pandemic. International Journal of Information Engineering and Electronic Business, 13(2). https://doi.org/10.5815/ijieeb.2021.02.01.

Rajkumar, P.V., et al. (2023). Cyber security and hybrid work environments. SAM Advanced Management Journal, 88(3).

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

Rogers, R.W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. J Psychol., 91(1): 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Russel, S. (1986). Privacy: History, legal, social, and ethical aspects and privacy: Its role in federal government information policy. Institute of Education Science, 35(1): 7–42.

Schulza, J., & Krumm, S. (2016). The "virtual team player": A review and initial model of knowledge, skills, abilities, and other characteristics for virtual collaboration. Organizational Psychology Review, 7(1). https://doi.org/10.1177/2041386616675522.

Shank, J. (1986). Technology as a Threat to Privacy.

Smith, H.J., Milberg, S.J., & Burke, S.J. (n.d.). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2): 167–196. https://doi.org/10.2307/249477.

Solove, D. (2015). Social dimensions of privacy. Cambridge University Press. https://doi.org/10.1017/cbo9781107280557.

Sorum, P., Stein, C., Wales, D., & Pratt, D. (2022). A Proposal to Increase Value and Equity in the Development and Distribution of New Pharmaceuticals. International Journal of Health Services, 52(3): 363–371. https://doi.org/10.1177/00207314221100647.

Sostero, M., Milasi, S., Hurley, J., & Mathias, E. (2023). Teleworkability and the COVID-19 crisis: Potential and actual prevalence of remote work across Europe. IZA Journal of Labor Policy. https://doi.org/10.2478/izajolp-2023-0006.

Soumelidou, A., & Tsohou, A. (2021). Towards the creation of a profile of the information privacy-aware user through a systematic literature review of information privacy awareness. Telematics and Informatics, 61: 101592. https://doi.org/10.1016/j.tele.2021.101592.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication, 19(2): 248–273. https://doi.org/10.1111/jcc4.12052.

Van, S., et al. (2006). Concern for Information Privacy and Online Consumer Purchasing. J. AIS. https://doi.org/10.17705/1jais.00092.

Vidhyaa, B., & Ravichandran, M. (2022). A literature review on hybrid work model. International Journal of Research Publication and Reviews.

Westin, A.F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2): 431–453.

Wirth, J. (2017). Strength of ties as an antecedent of privacy concerns: A qualitative research study. In Proceedings of the Twenty-Third Americas Conference on Information Systems (AMCIS), Boston, MA. AIS Electronic Library (AISeL). https://aisel.aisnet.org/amcis2017/informationsystems/presentations/13.

Wisniewski, P.J., & Page, X. (2022). Privacy theories and frameworks. Springer. https://doi.org/10.1007/978-3-030-82786-1.

Xu, H., Teo, H.H., Tan, B.C.Y., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. Management Information Systems Quarterly, 34(1): 135–174.

Zhou, T. (2011). Understanding online community user participation: A social influence perspective. Internet Research, 21(1): 67–81. https://doi.org/10.1108/10662241111104884.