Middle East Journal of Applied Science & Technology (MEJAST)
Volume 9, Issue 1, Pages 141-161, January-March 2026

Privacy Concerns with Bring Your Own Device in Virtual Teams: A view from remote workers in Mauritius

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

[1]*Researcher, Open University of Mauritius, Reduit, Mauritius.*
[2]*Associate Professor, University of Technology Mauritius, Pointe aux Sables, Mauritius.*
[3]*Academic, Open University of Mauritius, Reduit, Mauritius.*
Email: rooma.ramasamy@gmail.com[*]

DOI: Under Assignment

Article Received: 25 January 2026 *Article Accepted: 27 March 2026* *Article Published: 29 March 2026*

ABSTRACT

The future of work, that is working in virtual settings, introduces complex questions of privacy concerns and behaviours related to privacy in virtual environments including with Bring Your Own Devices (BYOD). Based on the Privacy Paradox and Concerns for Information Privacy (CFIP) scale, the study aims to provide an in-depth comprehension of how individuals face privacy concerns in the context of BYOD in virtual settings by analysing privacy through a multifaceted lens. The approach to disseminate the research question of this study included quantitative paradigms. Methods were survey questions, Data sets emerging from these instruments were analysed and presented to comprehend the phenomenon. The use of BYOD in virtual environment showed disparity with stated privacy concerns.

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

1. Introduction

Following the increasing use of the smartphone in the workplace, many organisations have adopted the practice of Bring Your Own Device (BYOD), acknowledging it positively maximises productivity (Downer and Bhattacharya, 2022). Global studies estimated that an average of 75% of organisations allow the use of mobile devices for work. In some sectors, as high as 85% of employees use personal devices to access work-related sensitive information. Even though BYOD has huge benefits, it also inherits risks that the traditional computers have including introducing additional risks such as unauthorised access, data breaches, data leak amongst others or in short privacy risks. Previous literature reviews and research focusing on the current state of BYOD revealed that BYOD security is still an under-researched concept (Downer and Bhattacharya, 2022).

BYOD is controlled by the users and is therefore subject to various threats. The employees are performing work for their organization on their device, which allows many risks of leakage or direct access to personal data (Kulkarni *et al.* 2014). A systematic literature review was conducted by Octavia *et al.* in 2016 and found security and privacy challenges which are data, device, network, malware, bandwidth, inconsistent security policy, leakage in shared media, readable data, inter-application data leakage, ownership, password, modify and damage records, and vandalize technical equipment (Octavia *et al.* 2016).

According to Ayedh *et al.* (2023), earlier research has not emphasized enough on security and privacy concerns from a BYOD perspective, especially crucial aspects of privacy such as anonymity, data protection, and user consent. The purpose of this paper is to examine privacy concerns related to BYOD among remote workers. The research aims to explore how individuals' privacy concerns relate to their actual privacy behaviours in a BYOD environment, assess generational differences in these behaviours, and identify any gaps between privacy awareness and behaviour.

The structure of this paper is as follows: Section 2 presents an in-depth literature review, followed by the methodology in Section 3. Section 4 includes the analysis and discussion of results, and Section 5 concludes with recommendations and final reflections.

1.1. Study Objectives

1) Examine the relationship between individuals' privacy concerns and their actual privacy behaviour in a BYOD environment.

2) Determine any significant difference in privacy behaviour among the working generation in a BYOD environment.

3) Examine any significant disparity between behaviour and awareness towards privacy concerns?

2. Related Works

2.1. BYOD in Virtual Teams

Traditionally, before the 1990s, organisations in traditional settings in face-to-face environments used phones, computers, printers, among others, as office equipment (Mamaghani, 2006). However, with innovation over the last decade, there has been a dramatic change in complementary technologies, that is, the smartphone. The organisation has therefore become flexible due to this phenomenon and has brought the concept of BYOD or also sometimes referred to as Bring Your Own Technology (BYOT). BYOD is an organizational strategy that can enhance efficiency and effectiveness by providing flexible access to essential company information, enabling employees to work from any location at any time, supporting social interaction among staff and stakeholders, and empowering employees in their roles. When this approach is well designed and executed, it is likely to gain support from both employees and employers. However, if it is poorly planned or implemented, BYOD can lead to adverse outcomes.

Employees are therefore able to use their devices in the workplace, such as their tablets, laptops, or mobile phones (Garba *et al.* 2015). BYOD has roots in several academic fields, including business and management and Information Systems (IS). Rosman *et al,* (2022) define BYOD as using one's device, facility, or gadget to perform organisational activities. Gustav and Kabanda (2016), on the other hand, perceive BYOD being a new technology adoption model where organisations provide their employees the facility to make use of their devices, to carry out work-related tasks such as email exchange, document processing, or remote connection to critical systems is even possible. Employees can access many work-related applications on their smartphones, such as mobile dashboards, company and employee contact information, and corporate mobile applications. On their smartphones, they can download professional documents as well. This increases the urgency of the problem of smartphone security (Ameen *et al.* 2021). Two out of every five employees, according to research by Symantec, download work files on their smartphones and tablets. Therefore, the use of mobile devices by employees exposes both business and personal data to a variety of security risks and data leaks (Symantec, 2015).

Despite some risks, enabling employees to bring and use their gadgets while at work also provides some benefits. To keep employees motivated, the device they use should be simple to operate. When employees use their phone, which they like and are familiar with, they are considerably happier at work (Gokce and Dogerlioglu, 2019). BYOD

provides the comfort of ease of access to the organisational network anytime and anywhere without the burden of an extra device (Morrow, 2012; Thomson, 2012). BYOD improves employee availability, which enhances their flexibility and mobility, in turn allowing them to work remotely with ease, contributing to business continuity (Doargajudhur, 2020).

They also have the opportunity not to be bound to their workspace whole day and may be able to work at any location (Madzima, Moyo, and Abdullah, 2014). BYOD also results in cost savings because employees bring their own devices for use by their employers, which reduces the need for initial device purchases, ongoing usage, and IT helpdesk support (Aguboshim and Udobi, 2019). Since BYOD devices are used for both personal and professional purposes, BYOD might restrict employees' use of their own devices by imposing rigorous constraints on the company. The right to select which application can be downloaded and installed does not belong to the user (Jaramillo, Ackerbauer, and Woodburn, 2014). They are also concerned about data privacy because the business has access to all personal information to remotely manage the gadget. Users may feel insecure as they think that there may be a possibility the organisation might have access to their private space (Wang, Wei, and Vangury, 2014). Inadequate security features on personal hardware may make privately owned computers vulnerable to cybersecurity attacks, which could result in several issues if they are given access to corporate information. Additionally, when personal devices when used for work, there is a probability of mixing business and personal information, which may increase the risk of inadvertent disclosure or data leakage (Ayedh *et al.* 2023). Once employees dispose of or sell their devices, any corporate data that was not completely deleted could be exposed to third parties (Rosman *et al.* 2022). Oktavia *et al.* (2016) in a systematic literature classified components of the security and privacy challenge as: data, device, network, malware, bandwidth, inconsistent security policy, leakage in shared media, readable data, inter-application data leakage, ownership, password, modify and damage records, and vandalize technical equipment.

2.2. BYOD and Privacy Concerns

Enabling employees to access company data on their own devices raises several questions that a firm must address to uphold its data protection duties (Aguboshim and Udobi, 2019). While information privacy is the responsibility of the user in BYOD as the unintended administrator, the device owner manages the following aspects of privacy:

- Physical Privacy: Freedom from unwanted/unwarranted touching or restriction of movement;
- Information privacy: fairness, transparency, and control related to information about people;
- Social privacy: The ability to associate with anyone who wishes to (HMG, 2018).

Organizations have had to embrace the trend of BYOD and not compromise on the issue of information privacy (Musarurwa *et al.* 2018). The need for a framework to ensure information privacy is important. Degirmenci *et al.* (2025) found that employees' attitudes toward the use of BYOD are negatively impacted by their perceived risks. Therefore, the greater concerns result in a less positive perception of BYOD. On the other hand, their attitude is favourably influenced by perceived benefits, with more benefits promoting a more positive view of BYOD adoption. It is therefore important to understand the use of BYOD in the virtual team setting and analyse privacy concerns, awareness, and behaviour.

3. Methodology and Data Analysis

This study adopted a quantitative, cross-sectional design from the lens of the privacy paradox to investigate working generation differences on privacy behaviours and the relationship between individual privacy concerns with the Bring Your Own Device contexts in virtual teams. To explore the relationship between privacy concerns and BYOD behaviours across the working generation, this study adopted the Concern for Information Privacy framework developed by Smith *et al.* (1996) as a guiding theoretical lens. The CFIP model is based on four dimensions: collection, unauthorized secondary use, errors, and improper access, representing a structure for understanding the respondents' perceptions of privacy practices.

A total of 154 individuals representing different working generations, Gen Z, Millennials, Generation X, and Baby Boomers were collected. The target population is individuals in the ICT industry known to be working in a virtual setting in Mauritius. To reach respondents from the ICT industry working in virtual settings, a purposive and snowball sampling approach was adopted considering the challenge in identifying the previously unknown population. Direct emails have been sent to organization members of the Outsourcing and Telecommunications Association of Mauritius (OTAM), and recruitment efforts was also done on LinkedIn. Selected participants were encouraged to refer their peers, allowing the population to expand but however maintaining the objectivity of the scope. A structured questionnaire using Likert scales based on CFIP dimensions were not used to shape the structure of privacy concerns measured in the study.

The Kolmogorov-Smirnov and Shapiro-Wilk tests were used to determine whether the continuous variables (Behaviour_BYOD, Concern_BYOD, and BYOD Frequency) were normal data. Non-parametric tests were appropriate due to the dataset's non-normality. For ordinal and skewed data, Spearman's rho, Chi-Square, and Kruskal-Wallis tests are commonly advised. The Spearman's rho correlation coefficient was used to investigate the relationship between individual's actual behaviour in a BYOD environment and their privacy concerns. Additionally, to determine whether age group and privacy behaviour levels correlated, a Chi-Square Test of Independence was used. The median behaviour scores for each age group were contrasted using the Kruskal-Wallis H test. Given the non-normal data and the dependent variable's ordinal nature, the test was appropriate.

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.

1) What is the relationship between individuals' privacy concerns and their actual privacy behaviour in a BYOD environment?
2) Is there a significant difference in privacy behaviour among the working generation in a BYOD environment?
3) What is the significance of behaviour and awareness towards privacy concerns?

4. Data Analysis and Discussion

4.1. Reliability

According to Saunders *et al.* (2009) commonly used thresholds for reliability tests are:

- $\alpha \geq 0.9$: Excellent reliability
- $0.8 \leq \alpha < 0.9$: Good reliability
- $0.7 \leq \alpha < 0.8$: Acceptable reliability
- $\alpha < 0.7$: Poor reliability

Reliability tests were conducted for each construct of this study, that is Behaviour and Concern.

A. Behaviour

Reliability Statistics

Cronbach's Alpha	N of Items
.862	5

Figure 1. Reliability Test for Variable Behaviour

A Cronbach Alpha of 0.862 as shown in Figure 1, therefore, suggests a good consistency among the items in the scale (Take a moment to consider when asked to provide personal information, read and understand the privacy policy of the apps they use for BYOD, share their BYOD with family members or friends, use MFA in their BYOD-related applications, connect to public Wi-Fi)

B. Concerns

A Cronbach Alpha of 0.942 as shown in Figure 2, therefore, suggests a good consistency among the items in the scale(concern about privacy issues related to mobile apps, concerned about sharing personal information with mobile apps, concerns about mobile apps sharing their personal information, believe their mobile device location is being monitored, concerned about mobile apps collecting too much information, concerned about mobile apps monitoring their activities, concern about personal data exposure, concern regarding personal data collection, personal information is being shared by mobile apps)

Reliability Statistics

Cronbach's Alpha	N of Items
.942	9

Figure 2. Reliability Test for Variable Concerns

4.2. Test of Normality

For the scale used to measure privacy concerns, different tests were conducted on the constructs as shown in Figure 3 and 4.

Tests of normality were carried out using the Shapiro-Wilk test across age groups. Descriptive statistics were computed for privacy behaviour and privacy concerns across Gen Z, Millennials, and Gen X. For Behaviour, Gen Z reported the highest mean, followed by Gen X. Skewness indicated a moderate positive skew for all generations. For Concerns, Gen X reported the highest, followed by Gen Z and Millennials with negative skew particularly for Gen Z, suggesting a tendency toward higher concern scores.

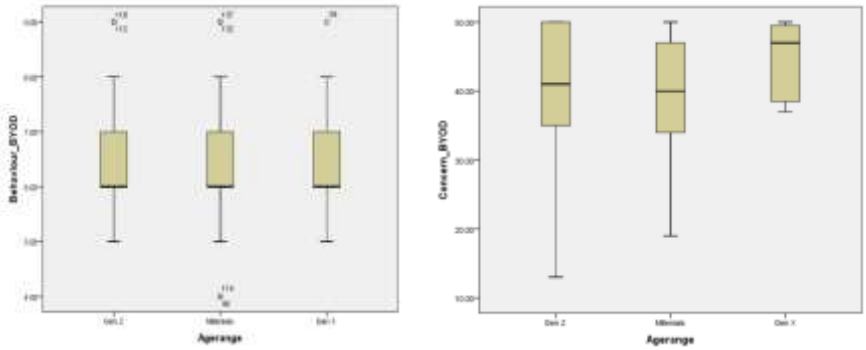

Figure 3. Test of Normality Behaviour and Concerns Age group

Normality tests indicated that the data were not normally distributed across groups, and variances were unequal. Given these deviations, the assumption of normality may not be fully met. Therefore, non-parametric statistical methods is appropriate for analysing the variables across age groups to ensure the validity of the results.

Additionally Baby Boomers were excluded due to low representation.

Case Processing Summary

		Cases					
		Valid		Missing		Total	
	Agerange	N	Percent	N	Percent	N	Percent
Behaviour_BYOD	Gen Z	25	86.2%	4	13.8%	29	100.0%
	Millenials	97	93.3%	7	6.7%	104	100.0%
	Gen X	19	82.6%	4	17.4%	23	100.0%
Concern_BYOD	Gen Z	25	86.2%	4	13.8%	29	100.0%
	Millenials	97	93.3%	7	6.7%	104	100.0%
	Gen X	19	82.6%	4	17.4%	23	100.0%

Figure 4. Case Base Processing Behaviour and Concerns Age group

4.3. Descriptive Statistics

A. Use of a personal device to access work-related applications

The descriptive statistics Figure 5 provides insights into the responses to the question "Do you use your personal device to access work-related applications?" A total of 156 participants working in virtual teams across various industries, including the ICT and BPO sectors. The survey consisted of Likert-scale-related question. The data shows that every single respondent answered with a '1', which corresponds to a "Yes" response.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Doyouuseyourpersonaldevicetoaccessworkrelatedapplicat	156	1	1	1.00	.000
Valid N (listwise)	156				

Figure 5. Descriptive Statistics Variable Use of BYOD

B. Demographics

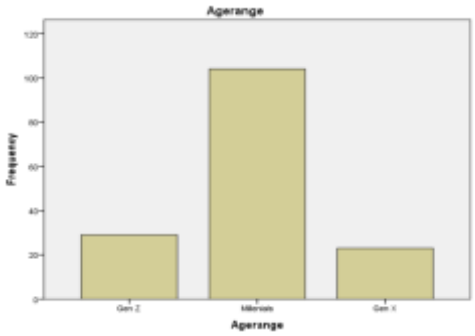

Figure 6. Demographics

The chart from Figure 6 shows that Millennials make up most of the surveyed population, significantly outnumbering both Gen Z and Gen X. Gen Z and Gen X are also represented. The sample group being analysed is predominantly composed of Millennials.

C. Frequency of use of BYOD

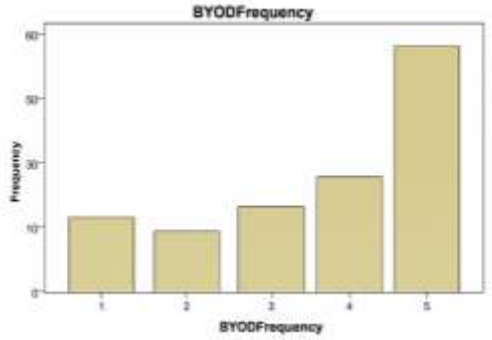

Figure 7. Frequency of use of BYOD

The chart in Figure 8 shows the frequency of use of BYOD represented by from 1 = Rarely to 5 being very frequent. Participants' use of personal devices for work varied across the sample. The majority reported using BYOD frequently. Lower frequencies were less common. Overall, most participants engaged in BYOD regularly, highlighting its prevalence in the virtual work environment. The standard deviation confirms that there is diversity in the participants' BYOD usage frequency. This could be important when analysing the relationship between BYOD frequency and other factors, such as privacy concerns.

D. Multi-Factor Authentication (MFA)

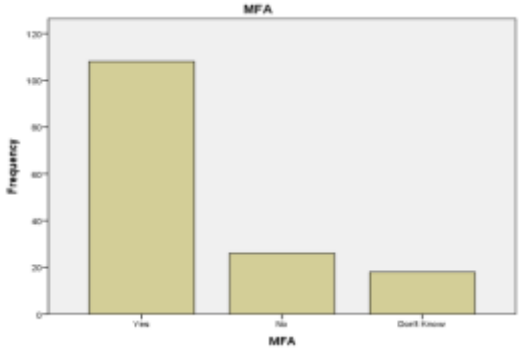

Figure 8. Frequence of Multi-Factor Authentication

The majority of respondents are using MFA in their BYOD-related applications, as shown in Figure 9, which is a good sign in terms of security practices. A small portion are not using MFA, and an even a smaller number of respondents are unsure whether MFA is in place. While these insights do confirm positive behaviour over protecting information over BYOD, the presence of users not having MFA in place indicates a potential lack of awareness which is a concern. If users are unaware of their security settings, they may not be taking adequate steps to protect sensitive data, increasing the risk of accidental data exposure.

E. Sharing BYOD with a family member

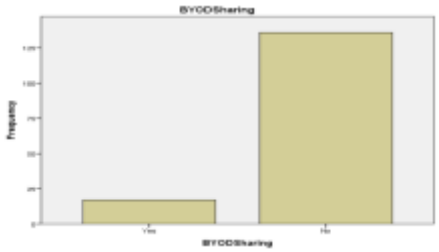

Figure 9. Frequence of BYOD sharing

Most respondents do not share their BYOD with family members or friends, as shown in Figure 10, which could suggest concerns about privacy or security. A small portion shares their BYOD, possibly indicating a greater trust or a more casual attitude toward security and privacy in their personal devices. While most users demonstrate caution by not sharing their devices, the minority who do share them may pose a privacy risk, highlighting the need for clear policies and user education on secure BYOD practices.

F. BYOD Privacy policy

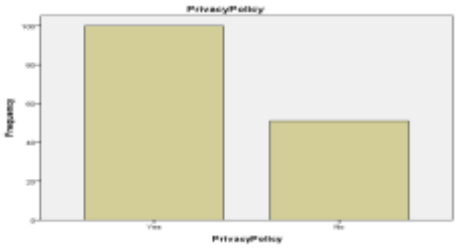

Figure 10. Frequence of BYOD Privacy policy

A majority of respondents read and understand the privacy policy of the apps they use for BYOD, as shown in Figure 10. This suggests that many are aware of privacy-related concerns when using personal devices for work-related tasks. A significant minority do not read or understand the privacy policies, which may indicate a potential security risk or lack of awareness.

G. Connection to Public Wifi

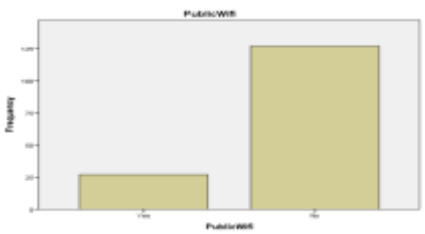

Figure 11. Frequence of connection to public Wifi

Most respondents as shown in Figure 11, avoid connecting to public Wi-Fi, possibly due to concerns over privacy and security risks associated with unprotected networks. A smaller portion connects to public Wi-Fi, which may indicate a greater sense of convenience or less concern about security risks in such environments.

H. Mobile apps may use personal information for other purposes without notifying me or getting my authorization

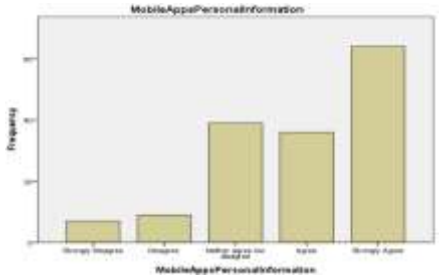

Figure 12. Frequence of use of personal information

A strong majority of respondents are inclined towards agreeing, as shown in Figure 12, indicating a high level of awareness and concern about privacy issues related to mobile apps. Only a small percentage strongly disagree or disagree, which suggests that concerns about personal data usage by apps are prevalent.

I. Concern about personal information with mobile apps

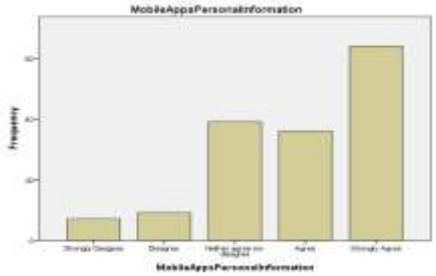

Figure 13. Frequence of concern with personal information

A large portion of respondents strongly agree that they are concerned about sharing personal information with mobile apps, suggesting high awareness of privacy risks as shown in Figure 13. Combining the agree and strongly agree categories shows that most respondents have some level of concern when providing personal information to mobile apps. Only a small percentage strongly disagree or disagree, indicating that most respondents are concerned, to some degree, about their personal data.

J. Take a moment to consider when asked to provide personal information

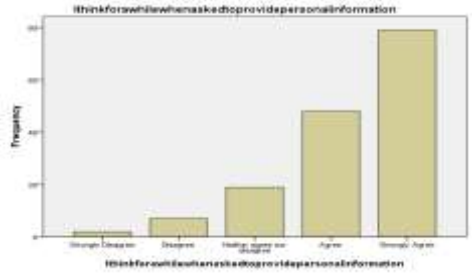

Figure 14. Frequence of Think before providing personal information

A strong majority of respondents agree or strongly agree that they think for a while before providing personal information, indicating a high level of caution and consideration regarding the sharing of personal data as shown in Figure 14. A minority strongly disagree or disagree, suggesting that they do not give much thought before sharing their personal information.

K. Personal information sharing on mobile apps

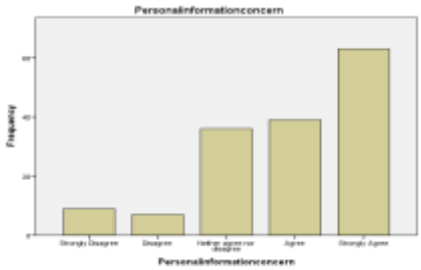

Figure 15. Frequence of Concerned about mobile apps sharing their personal information

A large portion of respondents as shown in Figure 15 agree or strongly agree that they have concerns about mobile apps sharing their personal information, suggesting a high level of concern about privacy and data security. Only a small percentage strongly disagree or disagree, indicating that very few people feel unconcerned about this issue.

L. Location monitoring on a mobile device

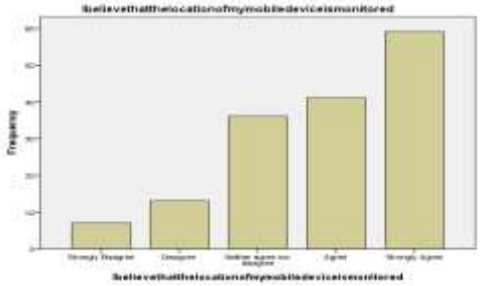

Figure 16. Frequence of Location monitoring on a mobile device

A majority of respondents as shown in Figure 16, agree or strongly agree that they believe their mobile device location is being monitored, showing a strong concern or awareness of location tracking. A smaller percentage strongly disagree or disagree, suggesting that some respondents are less concerned about or less aware of location tracking. The neutral category represents those who are unsure or indifferent about this issue. The data suggests that a significant number of respondents are concerned about the monitoring of their mobile device location, reflecting broader concerns about privacy and security.

M. Collection of information by mobile apps

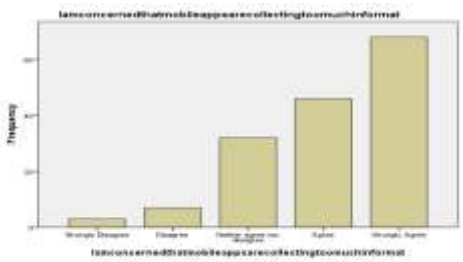

Figure 17. Frequence of Collection of information by mobile apps

A large portion of respondents as shown in Figure 17, agree or strongly agree that they are concerned about mobile apps collecting too much information. This indicates a strong awareness and concern regarding privacy issues. Only a small percentage strongly disagree or disagree, suggesting that a very few are unconcerned about the amount of data being collected. The data reveals that most respondents are worried about the level of information that mobile apps collect, which aligns with increasing concerns over personal data privacy and control.

N. Activity Monitoring on mobile apps

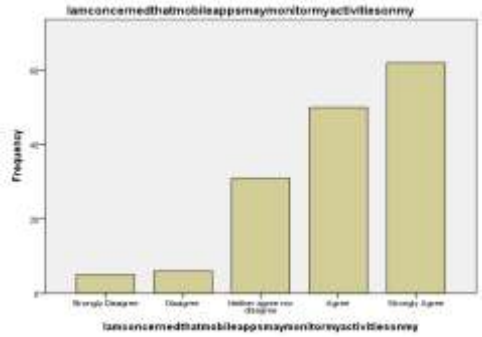

Figure 18. Frequence of activity monitoring on mobile apps

Most respondents as shown in Figure 18 agree or strongly agree that they are concerned about mobile apps monitoring their activities. This demonstrates a strong awareness of privacy concerns associated with mobile apps. A small percentage strongly disagree or disagree, indicating that only a few individuals are unconcerned about activity monitoring by mobile apps. A considerable portion is neutral, suggesting that some people may be unsure about the extent to which mobile apps monitor their activities. Many respondents have concerns about mobile apps monitoring their activities, which reflects growing concerns over privacy and tracking in the digital world.

O. Personal information when using mobile apps

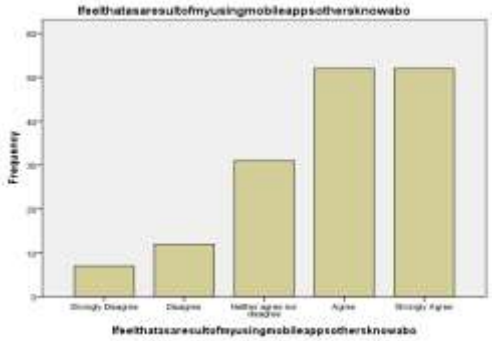

Figure 19. Frequence of Personal information with the use of mobile apps

Majority of respondents as shown in Figure 19 agree or strongly agree that they feel others may be aware of their personal information because of using mobile apps, indicating a strong concern about personal data exposure. A smaller group strongly disagrees or disagrees, suggesting that only a few individuals are unconcerned about the privacy risks of mobile apps. 22.4% remain neutral, meaning some respondents may be unsure or unaware of how mobile apps could potentially expose their personal information. Most respondents are concerned about the exposure of their personal information through mobile apps, highlighting an ongoing awareness of privacy issues in the digital world.

P. Readily available information with the use of mobile apps

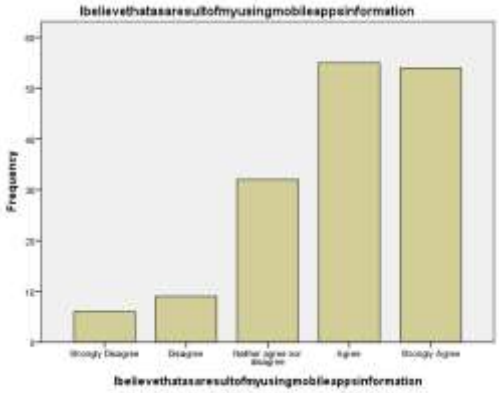

Figure 20. Frequence of Use of mobile apps has made private information more readily available to others

Most respondents shown in Figure 20 agree or strongly agree that they believe information is being collected about them due to their use of mobile apps. This highlights a significant concern regarding personal data collection. A low number of respondents disagree or strongly disagree, suggesting that they don't believe their information is being collected. The remaining are neutral, indicating uncertainty or lack of awareness about the data collection practices of mobile apps. Most respondents believe mobile apps are collecting their information, reflecting growing awareness and concern about privacy and data usage in the mobile app ecosystem.

Q. Privacy invasion

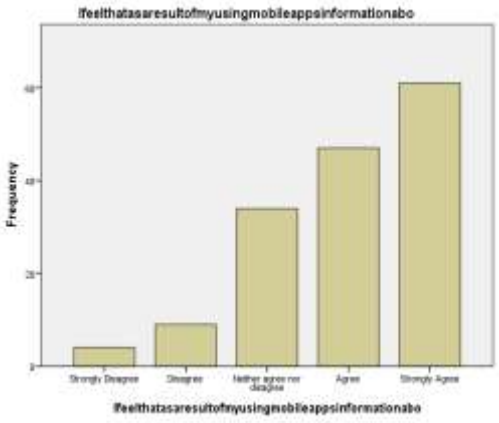

Figure 21. Frequence of Privacy invasion

Majority of respondents as shown in Figure 21 agree or strongly agree that they feel their personal information is being shared by mobile apps. This shows a high level of concern about information sharing. A low number of respondents disagree or strongly disagree, meaning a smaller group does not feel their information is being shared. The medium neutral responses, indicating uncertainty or indifference about sharing their data with mobile apps. The majority of respondents feel that mobile apps are sharing their information, indicating a widespread concern about privacy and data sharing practices in mobile applications.

R. Common BYOD Devices

The devices used was surveyed, with Mobile phone leading at 76.3%, followed by personal Laptop (43.7%), tablet (9.6%) and wearables at 13.3%.

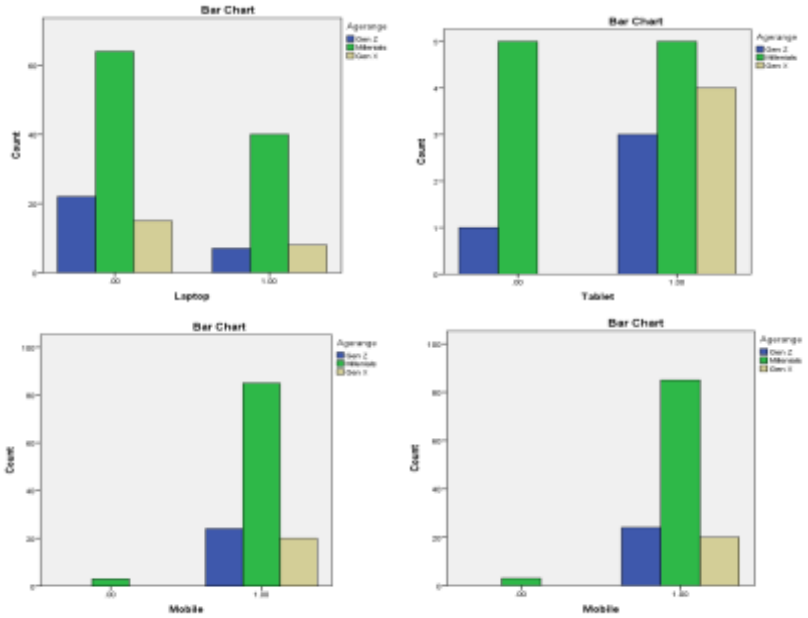

Figure 22. Analysis devices

Figure 22 shows that mobile devices were the most widely adopted, with 129 participants across all generations reporting usage of BYOD, indicating that smartphones are the dominant BYOD tool. Laptop was also prevalent with 55 respondents claiming use. Wearables smartwatches had limited adoption, with only 14 users, mostly among Millennials. Overall, the findings highlight that while mobile devices are the primary tool for BYOD across all generations, laptops remain common, whereas tablets and wearables show much lower uptake. These findings align with recent literature on generational differences in technology use within virtual teams. Consistent with studies by Ferrara *et al.* (2017) and Wang and Duan (2024), Millennials in this study represent the highest proportion of users across all device types, indicating a greater integration of digital tools in their virtual work practices.

S. Common applications of BYOD

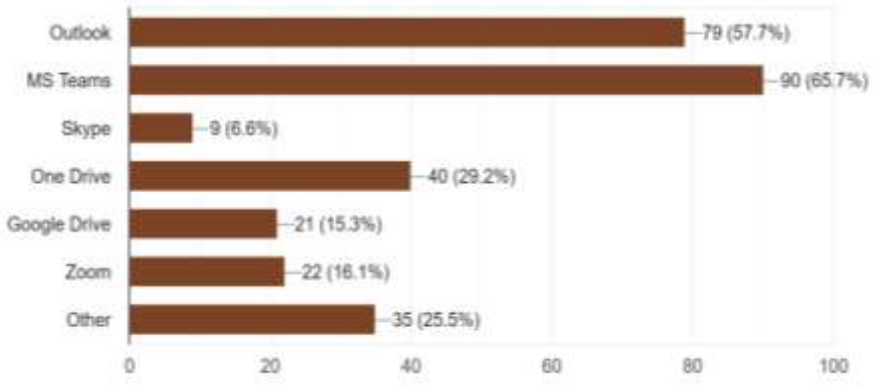

Figure 23. BYOD applications percentage

The use of applications accessed from BYOD is detailed in Figure 23. Participants who responded were mostly using Outlook, MS Teams, OneDrive, Zoom, Google Drive, and Skype. The number of responses varied considerably across tools, with MS Teams and Outlook receiving the highest number of responses. In contrast, tools such as Skype and Google Drive had notably lower response rates. To note that Microsoft retired the Skype application in May 2025.

4.4. Hypothesis Testing

To examine the impact of Bring Your Own Device (BYOD) practices across generations, hypothesis testing was conducted on the relationship between constructs and working generation groups. The analysis aimed to determine whether significant differences exist in privacy concerns and behaviour with BYOD among Gen Z, Millennials, and Gen X.

A. Privacy Concerns and Behaviour

H01: There is no statistically significant relationship between individuals' privacy concerns and their actual behaviour in a BYOD environment.

Correlations

			Behaviour_BYOD	Concern_BYOD
Spearman's rho	Behaviour_BYOD	Correlation Coefficient	1.000	.169*
		Sig. (2-tailed)		.045
		N	151	142
	Concern_BYOD	Correlation Coefficient	.169*	1.000
		Sig. (2-tailed)	.045	
		N	142	149

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

Figure 24. Correlation Privacy Concerns / Behaviour

The relationship as shown in Figure 24 between respondents' actual behaviour with BYOD and their privacy concerns was examined using Spearman's rank correlation. The weak positive correlation ($r = 0.169$, $p = 0.045$) suggests that respondents with greater privacy concerns are more likely to be cautious with their BYOD. Therefore, at the 0.05 level, the correlation was statistically significant.

The null hypothesis can therefore be rejected.

B. Concern Behaviour / Demographics

H02: There is no significant association between generational age group and privacy behaviour and concern in a BYOD environment.

A Kruskal Wallis test as shown in Figure 25, was conducted to examine whether behaviour and concerns differ across age groups of Gen Z, Millennials and Gen X. Results indicate that there is no statistically significant difference in either behaviour or concern across age categories. While concern levels showed a p-value close to significance, it did not cross the 0.05 threshold, suggesting that generational differences in concerns may exist but were not strong enough.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Behaviour_BYOD is the same across categories of Agerange.	Independent-Samples Kruskal-Wallis Test	.235	Retain the null hypothesis.
2	The distribution of Concern_BYOD is the same across categories of Agerange.	Independent-Samples Kruskal-Wallis Test	.076	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Figure 25. Kruskal Wallis test on Behaviour / Demographics

Test Statistics

	Agerange	Behaviour_BYOD	Concern_BYOD
Chi-Square	78.346[a]	177.920[b]	147.605[c]
df	2	5	30
Asymp. Sig.	.000	.000	.000

a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 52.0.

b. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 25.0.

c. 31 cells (100.0%) have expected frequencies less than 5. The minimum expected cell frequency is 4.7.

Figure 26. Behaviour / Demographics

Therefore, to dive deeper, Kendall's tau-b, Spearman's Rank, and were run as shown in Figure 27.

Correlations

			Agerange	Concern_BYOD
Kendall's tau_b	Agerange	Correlation Coefficient	1.000	.065
		Sig. (2-tailed)	.	.327
		N	157	148
	Concern_BYOD	Correlation Coefficient	.065	1.000
		Sig. (2-tailed)	.327	.
		N	148	148
Spearman's rho	Agerange	Correlation Coefficient	1.000	.078
		Sig. (2-tailed)	.	.345
		N	157	148
	Concern_BYOD	Correlation Coefficient	.078	1.000
		Sig. (2-tailed)	.345	.
		N	148	148

Figure 27. Correlation Working generation / Behaviour and Concerns

The correlation analysis between age range and concern about BYOD revealed weak and statistically non-significant relationships. Kendall's tau-b has a correlation coefficient of .065 (p = .327), while Spearman's rho produced a slightly higher coefficient of .078 (p = .345). Both values indicate a very weak positive association between age and concern about BYOD, and the p-values suggest that these correlations are not statistically significant. Therefore, there is no meaningful relationship between age group and concern levels regarding BYOD in this sample.

The null hypothesis is therefore accepted.

To have additional insights, the variable frequency of use of BYOD was introduced. The correlation analysis reveals a statistically significant but modest positive relationship between frequency of using BYOD Frequency and their level of concern regarding BYOD. Both Kendall's and Spearman's rho indicate that as respondents engage more frequently in BYOD practices, their concerns about potential risks or implications tend to increase slightly. Although the strength of the correlation is weak, its consistency across both methods suggests a meaningful trend worth noting.

Correlations

			Concern_BYOD	BYODFrequency
Kendall's tau_b	Concern_BYOD	Correlation Coefficient	1.000	.127*
		Sig. (2-tailed)	.	.043
		N	148	145
	BYODFrequency	Correlation Coefficient	.127*	1.000
		Sig. (2-tailed)	.043	.
		N	145	154
Spearman's rho	Concern_BYOD	Correlation Coefficient	1.000	.175*
		Sig. (2-tailed)	.	.036
		N	148	145
	BYODFrequency	Correlation Coefficient	.175*	1.000
		Sig. (2-tailed)	.036	.
		N	145	154

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

Figure 28. Correlation Frequency / Concerns

C. Privacy Behaviour and Demographics

H03: There is no significant association between generational age group and privacy behaviour in a BYOD environment.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Behaviour_BYOD is the same across categories of Agerange.	Independent-Samples Kruskal-Wallis Test	.235	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Figure 29. Hypothesis Working Generation / Behaviour

Kruskal–Walli's test was run as showed in Figure 29, which showed no statistically significant differences in behaviour (p = .235) across working generation categories. These results suggest that behaviour is not significantly different across generations in this study.

A chi-square test as shown in Figure 31 was run to assess the independence of the generational group with privacy behaviour. The Chi-Square test results show no significant association between the variables, as all p-values are well above the 0.05 threshold.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Behaviour_BYOD * Agerange	150	96.2%	6	3.8%	156	100.0%

Figure 30. Working Generation / Behaviour Case Base

Overall, Millennials appear to consistently exhibit privacy behaviours. However, this may be due to sample limitations.

Behaviour_BYOD * Agerange Crosstabulation

Count

		Agerange			Total
		Gen Z	Millenials	Gen X	
Behaviour_BYOD	4.00	0	3	1	4
	5.00	1	5	2	8
	6.00	12	59	10	81
	7.00	7	24	5	36
	8.00	4	8	3	15
	9.00	2	3	1	6
Total		26	102	22	150

Figure 31. Crosstabulation Behaviour BYOD Age range

Based on the Kruskal-Wallis's test, there are no significant differences in the privacy behaviour across the four generational workforces, as indicated by the p-value of 0.358. This suggests that generational age group might not be a strong factor influencing privacy behaviour with BYOD in virtual teams.

The null hypothesis can be accepted.

To have additional insights, the variable frequency of use of BYOD was introduced. The correlation analysis shown in Figure 32 between BYOD Frequency and Behaviour BYOD reveals a weak and statistically non-significant relationship. Both p-values exceed the threshold of 0.05, indicating that the observed associations are not statistically significant. This suggests that the frequency with which individuals use their own devices does not relate to their behavioural patterns in BYOD contexts. In practical terms, using personal devices more often does not appear to influence how respondents behave with BYOD.

Correlations

			BYODFrequency	Behaviour_BYOD
Kendall's tau_b	BYODFrequency	Correlation Coefficient	1.000	.069
		Sig. (2-tailed)	.	.316
		N	154	149
	Behaviour_BYOD	Correlation Coefficient	.069	1.000
		Sig. (2-tailed)	.316	.
		N	149	151
Spearman's rho	BYODFrequency	Correlation Coefficient	1.000	.090
		Sig. (2-tailed)	.	.273
		N	154	149
	Behaviour_BYOD	Correlation Coefficient	.090	1.000
		Sig. (2-tailed)	.273	.
		N	149	151

Figure 32. Correlation Behaviour / Frequency of BYOD

According to the findings of this study, individuals who express greater privacy concerns also tend to be slightly more cautious when using their personal devices for professional purposes. Although being statistically significant, the correlation's modest strength points to factors other than privacy concerns such as frequency of use probably influencing behaviour with BYOD in a virtual setting. Additional variables, such as convenience, social influence, or perceived low risk, could encourage respondents to continue using personal devices for work even while they are aware of the possible privacy risks (Jin and Hsu, 2020). While it comes to BYOD, the necessity for more accessibility and flexibility often prevails over concerns about data security (Peppet, 2014). The findings from the study also align with the view of the Concern for Information Privacy (CFIP) framework by Smith *et al.* (1996). These findings can be justified by the Privacy Paradox theory, with BYOD, respondents may express privacy concerns, but their actual behaviour such as like disclosing private information on their devices may not match these concerns. Considering respondents from various generations may indicate identical behaviour that contradict their expressed concerns, the privacy paradox may be considered to explain why there is no correlation between privacy concerns and age group. According to a study conducted by Lutz and Ranzini (2021), the Privacy Paradox is apparent when there is convenience such as having easy access to work-related apps on personal devices on the go are thought to outweigh privacy concerns. Studies on digital natives and older generations have shown that, despite age differences in the perceived value of privacy, privacy concerns often fall to the sideline when convenience and usefulness are given priority (Kokolakis, 2021). Younger generations, who have grown up with technology, may be particularly susceptible to this paradox and disregard the risks when sharing data on personal devices. However, because of their lack of awareness or dependence on work-related processes, older generations may be cautious but nevertheless engage in behaviour that put their privacy at threat.

5. Recommendations, Conclusion & Future Direction

The relationship between individuals' behaviour and their privacy concerns regarding ICT in general, from a Privacy Paradox perspective, using the Concern for Information Privacy (CFIP) framework as a basis. Privacy concerns are expected to influence behaviour. The Privacy Paradox states that there is often a gap between what individuals express in terms of concern and how they act in practice (Kokolakis, 2017).

From this study, correlation tests were conducted to determine the relationship between self-reported concern for privacy and ICT-related privacy behaviour. The findings revealed a statistically significant but weak correlation, as indicated by Spearman's rho = 0.232, $p < 0.01$, confirming a gap between concern and behaviour. Although respondents reported high privacy concern, particularly around dimensions like unauthorised secondary use and improper access, this concern did not strongly translate into their actual behaviours.

According to the findings of this study, individuals who express greater privacy concerns also tend to be slightly more cautious when using their personal devices for professional purposes. Although statistically significant, the correlation's modest strength suggests that factors other than privacy concerns likely influence behaviour with BYOD in virtual settings. The weak correlation observed from the Spearman rho test may be linked to the CFIP framework, where a respondent may express high concern on questions around unauthorised secondary use for example as fears of their data being sold or reused without consent therefore reflecting concern. Still, however, being indifferent toward data collection practices, such as cookies. Similarly, concern about improper access, especially relating to personal or sensitive information, has been expressed as strong. The concern across CFIP dimensions underscores the complexity by linking general privacy concerns to behaviour. Supported by Barth and de Jong (2017), users' subjective risk overview and emotional responses vary significantly, reinforcing the Privacy Paradox. The study's findings regarding BYOD also align with the Concern for Information Privacy (CFIP) framework by Smith *et al.* (1996), highlighting four key areas of concern: data collection, unauthorized secondary use, improper access, and data errors. In the BYOD context, this perspective allows us to understand the rationale behind why privacy concerns do not always result in protective behaviours. Respondents may show concerns of the extent of data collection on their BYOD; however, these concerns are often overridden by convenience, workplace expectations, or on perceived necessity. The secondary use of information, another dimension of the scale where data initially collected for professional purposes could be repurposed or shared without the consent of the user, also aligns with the respondent's unease, even if their behaviour suggests trust in organizational safeguarding measures.

Meanwhile, concerns about data errors and organizational responsibility for maintaining accurate records on personal devices appeared important, possibly due to limited awareness or perceived control. Overall, CFIP provides a foundation to observe the disconnect between attitudes and actions, supporting the findings that privacy concerns are often subjective, have contextual pressures, and the broader narrative identities individuals construct in navigating professional and personal digital boundaries. The finding from this study supports the concept that privacy concerns and actual behaviour in BYOD environments may not always be aligned. The findings also suggest that the working generation, and the variables privacy behaviour and privacy concerns do not have a statistically meaningful link. Therefore, although the differences between the workplace generation, their privacy-related concerns and behaviours regarding BYOD are aligned. These results align with previous studies,

also indicating that generational differences do not significantly distinguish privacy concerns in digital environments. For example, Taddicken (2020) found that although younger generations are more technology savvy, when contextual factors such as perceived risks and trust are considered, their privacy concerns are frequently the same as those of older generations. This questions that fact that because younger generation use technology more often, they are less concerned about privacy. The findings from Pearson's R, Spearman's Rank, including Kendall's tau-b did not also demonstrate any meaningful associations between age group and privacy behaviour. Privacy behaviour is more complex, factored by other variables other than by generational age. There is consistency with previous research indicating, not only generational influence privacy attitudes but also other elements.

In terms of future directions, it is proposed to:

Test privacy concerns and behaviour with BYOD in different environments to assess contextual variations in user responses conduct longitudinal studies to compare user insights before and after reading disclaimers and clicking "Agree." Embed privacy by design in mobile applications software development include the variable gender.

Declarations

Source of Funding

This study did not receive any grant from funding agencies in the public, commercial, or not–for–profit sectors.

Competing Interests Statement

Authors have declared no competing interests.

Consent for publication

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

Institutional Review Board Statement

Not applicable for this study.

Informed Consent

Not applicable for this study.

References

Aguboshim, F.C., & Udobi, J.I. (2019). Security issues with mobile IT: a narrative review of bring your own device (BYOD). Information Technology (IT), 8(1).

Ayedh, M., Wahab, A.W.A., & Idris, M.Y.I. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: state of the art and future directions. Applied Sciences, 13: 8048. https://doi.org/10.3390/app13148048.

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): 525–554. https://doi.org/10.25300/misq/2019/14358.

Degirmenci, K., Breitner, M.H., Nolte, F., & Passlick, J. (2023). Legal and privacy concerns of BYOD adoption. Journal of Computer Information Systems. https://doi.org/10.1080/08874417.2023.2259346.

Downer, K., & Bhattacharya, M. (2022). BYOD security: a study of human dimensions. Informatics, 9(1): 16. https://doi.org/10.3390/informatics9010016.

Gerber, N., Stöver, A., & Marky, K. (2023). Human factors in privacy research. Springer.

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.

Jaramillo, D., Ackerbauer, M., & Woodburn, S. (2014). A user study on mobile virtualization to measure personal freedom vs. enterprise security. In Proceedings of the IEEE SECON, Pages 1–5. https://doi.org/10.1109/secon.2014.6950672.

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.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: 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.

Lam, H., Beckman, T., & Harcourt, M. (2025). Bring your own device (BYOD): organizational control and justice perspectives. Employee Responsibilities and Rights Journal, 37: 473–491. https://doi.org/10.1007/s10672-024-09498-1.

Lang, P.M. (2021). Privacy concerns and behavioural intentions in the digital age: a review of literature. Cyberpsychology, Behavior, and Social Networking, 24: 338–346. https://doi.org/10.1089/cyber.2021.0052.

Lutz, C., Hoffmann, C.P., & Ranzini, G. (2016). Privacy cynicism: a new approach to the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(4): 7. https://doi.org/10.5817/cp2016-4-7.

Mamaghani, F. (2006). Impact of information technology on the workforce of the future: an analysis. International Journal of Management, 23: 845.

Martin, K., & Shilton, K. (2020). Why experience matters to privacy: how context-based experience moderates consumer privacy expectations for mobile applications. Journal of the Association for Information Science and Technology, 71(8): 940–953. https://doi.org/10.1002/asi.23500.

Musarurwa, A., Flowerday, S., & Cilliers, L. (2018). An information security behavioural model for the bring-your-own-device trend. South African Journal of Information Management, 20(1): 1–9. https://doi.org/10.4102/sajim.v20i1.980.

Oktavia, T., Yanti, H.P., & Meyliana (2016). Security and privacy challenge in bring your own device environment: a systematic literature review. In Proceedings of the International Conference on Information Management and Technology (ICIMTech), Pages 194–199. https://doi.org/10.1109/icimtech.2016.7930328.

Padden, A. (2020). Privacy in the workplace: examining the role of narrative identity and personal data distinctions. Journal of Business Ethics, 165: 657–670. https://doi.org/10.1007/s10551-019-04189-7.

Rosman, M.R.M., Baharuddin, N.S., Alimin, N.A., Rosli, N.N.I.N., Shukry, A.I.M., & Razlan, N.M. (2022). Device (BYOD) and productivity: a conceptual framework. Proceedings, 82(1). https://doi.org/10.3390/proceedings2022082010.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students (5th Ed.). Pearson Education Limited.

Smith, H.J., Milberg, S.J., & Burke, S.J. (1996). Information privacy: measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2): 167–196. https://doi.org/10.2307/249477.

Stern, M. (2022). The privacy paradox revisited: exploring the relationship between privacy concerns and online behaviour. Journal of Privacy and Confidentiality, 12: 31–46. https://doi.org/10.29012/jpc.2022.12.1.31.

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.

Wang, Y., Wei, J., & Vangury, K. (2014). Bring your own device security issues and challenges. In Proceedings of the Consumer Communications and Networking Conference (CCNC), IEEE.