journalism and media

MDPI

Article

Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region

Walaa Bajnaid [1,*] and Shuaa Aljasir [2]

[1] Department of Marketing Communication, Faculty of Communication and Media, King Abdulaziz University, Jeddah, Saudi Arabia
[2] Department of Journalism and Digital Media, Faculty of Communication and Media, King Abdulaziz University, Jeddah, Saudi Arabia; shaljasir@kau.edu.sa
* Correspondence: wnbajnaid@kau.edu.sa

Abstract: This study examines the correlation between Online Privacy Literacy (OPL) and privacy protection behaviour (PPB), including evidence of any correlation between the two. In addition, it considers whether factors of intention, attitude, perceived behaviour, subjective norms, and perceived behaviour control mediate the relationship between OPL and PPB online, and whether the relationships between demographic variables may act as moderators. This research took a sequential mixed-methods approach, with Study One employing an online survey of 1040 voluntary digital media users in the Middle East and North Africa (MENA), and Study Two undertaking online interviews with ninety-five participants. The results found a relationship between OPL and PPB. In addition, subjective norms and perceived behaviour control also mediate relationship between OPL and PPB in MENA. Furthermore, while all the participants revealed paradoxical attitudes to PPB, the empirical study highlighted that the male participants tended to demonstrate greater concerns in relation to OPL.

Keywords: privacy; privacy literacy; privacy protection behaviour; planned behaviour; digital media

check for updates

Academic Editor: Andreu Casero-Ripollés

Received: 13 October 2024
Revised: 17 December 2024
Accepted: 28 December 2024
Published: 9 January 2025

Citation: Bajnaid, W., & Aljasir, S. (2025). Does Online Privacy Literacy Affect Privacy Protection Behaviour? A Mixed-Methods Study of Digital Media Users in the MENA Region. *Journalism and Media*, *6*(1), 8. https://doi.org/10.3390/journalmedia6010008

1. Introduction

Digital media interactions now form a central aspect of daily life across the regions of the Middle East and North Africa (MENA). This lifestyle may expose users to several risks and raise concerns about violations of users' privacy. Such concerns have led to a number of studies being undertaken within the region to address privacy issues. A report by Consumers International (2019) revealed that MENA citizens are among the most concerned in the world about their online privacy and how their data are collected. In addition, a study by Northwestern University in Qatar involving seven countries of the MENA region found that four out of ten people were concerned about surveillance and their privacy. Such concerns led to changes in their behaviour on social media; for example, they changed their privacy settings, posted less information, stopped using their real names, and even ceased using some online services altogether (Dennis et al., 2019). Despite the widespread prevalence of such concerns, it should be noted that privacy is understood and perceived differently across social, cultural, economic, and political contexts (Masur et al., 2023).

MENA countries share significant similarities with respect to their geographies, cultures, religions, histories, and languages. Collectivism is the main cultural characteristic

across the region, emphasising the significance of the family or group image and harmony (Farooq et al., 2024). In addition, Arab countries are still among the most conservative societies and remain culturally concerned about women's public presence and family names (Sabbah & Sabbah, 2023), especially the Gulf countries (Farooq et al., 2024). However, MENA countries have demonstrated some differences in their dialects and cultures, which remain influenced by localised traditions. For instance, Dennis et al. (2019) found that internet users in some MENA cosuntries are more worried about institutional surveillance than that of the government. However, a report by Rassed (2014) found that the North African part of the region generally exhibits more trust in the idea that their personal data are safe on the internet and are more open to sharing information in public than those in the Gulf part. However, almost half of the individuals surveyed in both MENA parts believed that government censored content would protect users in many cases. Although not all MENA populations are Muslim, the Islamic religion has greatly influenced the Arabic norms that have influenced how privacy is understood (Abokhodair & Vieweg, 2016; Akour et al., 2022).

Various cross-culture studies have identified variations in privacy management practices among digital users (Colnago et al., 2023; Kaya & Yaman, 2021; Trepte et al., 2017; Vannucci et al., 2020). Moreover, Petronio and Altman (2002) emphasised that the context of individuals' daily lives, including the meanings attached to privacy, can exert a significant impact on attitudes to privacy. Several researchers have proposed that cultural norms can influence the importance a population places on privacy, employing the four national culture indicators developed by Hofstede (2011):s "individualism, power distance, uncertainty avoidance, and masculinity". In addition, Cho et al. (2023) stated that those living in individualistic cultures tend to place a greater importance on privacy than collectivistic societies, which are more amenable to both groups and organisations intruding on personal space. This suggests that users from Eastern countries are likely to be less concerned about online privacy than those from Western societies. The literature also indicates that prior research into privacy protection behaviour and users' privacy literacy levels has tended to focus primarily on Western and Eastern users (e.g., Obar & Oeldorf-Hirsch, 2020; Zeng et al., 2021; Lei et al., 2020).

Online privacy protection measures are generally associated with Internet-literate users (Kaya & Yaman, 2021). Online Privacy Literacy (OPL) is defined as the awareness of the ability to change privacy settings, as well as having the technical skills to undertake measures including hiding personal isnformation and limiting/restricting access to a social media account or profile (Masur, 2020). Thus, the number of previous studies indicates that OPL is related to privacy protection behaviour (PPB) (Afif et al., 2023; Baruh et al., 2017; Desimpelaere et al., 2020; Lund & Agbaji, 2023; Masur, 2020; Sindermann et al., 2021; Trepte et al., 2015). Desimpelaere et al. (2020) demonstrated that an individual's level of privacy literacy determines how much personal information they are willing to disseminsate. It is assumed that users with high levelss of OPL are familiar with privacy protection tools and aware of institutional surveillance and policy, and are, therefore, more likely to exercise information control (Park, 2013). This led the current researcher to examine the relationship between OPL and PPB.

Li et al. (2019) highlighted that a key component of PPB relates to an individual's intention to protect their privacy. In addition, Sadaf and Gezer (2020) demonstrated the link between digital literacy and digital performance, along with intention. Moreover, a study conducted by Baruh et al. (2017) found that OPL demonstrated a positive relation to the management of privacy, intention, and behaviour. In addition, the relationship between behaviour and intention has been highlighted by the Theory of Planned Behaviour (TPB), which, as noted by several studies, controls PPB (Alkhalifah & Alghafis, 2022; Dincelli &

Goel, 2015; Schäwel, 2018). However, intention is influenced by a number of variables, including attitudes towards performance, subjective norms relating to performance, and perceived control over behaviour (Li et al., 2019). Dincelli and Goel (2015) reported that privacy behavioural intention is preceded by Internet literacy, alongside subjective norms and privacy concserns. Various researchers (Bartsch & Dienlin, 2016; Debatin et al., 2009; Trepte et al., 2015) have argued that Internet users generally demonstrate an intention to act to combat privacy risks, but are prevented by their lack of knowledge. Unlike other theories related to PPB (e.g., privacy calculus theory and control agency theory), TPB views norms as constituting a key factor in the processing action, playing a major role in the context of MENA countries. This led us to re-examine the relationship between PPB and OPL, intention, perceived behaviour control, and subjective norms in the context of the MENA region.

Therefore, this study seeks to fill this gap in the literature as follows. Firstly, by expanding our understanding of the effects of users' privacy literacy on privacy protection behaviour online. Secondly, by exploring the factors influencing the relationship between OPL and PPB. Thirdly, by determining whether factors influencing behaviour (e.g., intention, attitude, perceived behaviour, subjective norms, and perceived behaviour control) tend to mediate the relationship between OPL and the protection of online privacy behaviours. This research, therefore, addresses the following research questions:

- RQ1: What is the relationship between the OPL and PPB of users in the MENA region?
- RQ2: What are the factors influencing the relationship between privacy literacy and privacy concerns?

2. Theoretical Background and Conceptual Model

TPB is an extension of the Theory of Reasoned Action (TRA), which focuses on the prediction of behaviour based on intention (Alkhalifah & Alghafis, 2022), conceptualised by the assumption that behaviour translates silent beliefs or intentions (Sadaf & Johnson, 2017). TPB postulates that behaviour is determined by intention and is influenced by three main factors: firstly, attitude (linked to behavioural beliefs); secondly, subjective norms (linked to normative beliefs); and, thirdly, perceived behaviour control (linked to control beliefs) (Dincelli & Goel, 2015; Sadaf & Johnson, 2017).

2.1. Intention

Sadaf and Gezer (2020) and Ajzen and Fishbein (1980) defined intention as the likelihood that an individual will engage in a specific behaviour, with Ajzen (1991) noting that "Intentions are assumed to capture the motivational factors that influence behaviour that indicate how hard people are willing to try and how much effort they are planning to exert, in order to perform the behaviour" (p. 181). Ajzen (1991) identified a significant positive correlation between the intention to disclose information on the Internet and privacy concerns, while Baruh et al.'s (2017) meta-analysis review of online privacy concern and privacy management showed a positive relationship between OPL and both intention and privacy protection behaviour. The current study assumes that OPL levels influences intention, which is then translated into privacy protection behaviours.

2.2. Attitudes

Attitudes refer to views of engaging in a particular behaviour (Ajzen, 1991), in which a positive or negative attitude arises as a consequence of behavioural beliefs (Uzun & Kilis, 2020). Ho et al. (2017) and Machuletz et al. (2018) found that positive attitudes were linked to increased engagement. On the other hand, Spiekermann et al. (2001) revealed discrepancies in protection behaviours, i.e., the privacy paradox. Furthermore,

Dienlin and Trepte (2015) divided approaches to privacy into three types (informational, social, and psychological), identifying that only psychological privacy demonstrated a negative impact on privacy protection behaviour. Moreover, Debatin et al. (2009) and Tsay-Vogel et al. (2018) focused on the link between the privacy attitudes and usage of Facebook users, revealing that they used this platform to socialise and, therefore, showed a relaxed attitude towards privacy.

2.3. Subjective Norms

Subjective norms refer to an individual's perception of other peoples' views of whether a behaviour should be performed, or the issue of social pressure, in which normative beliefs lead to subjective norms (Uzun & Kilis, 2020). Previous studies have found that subjective norms are the most important motivators of privacy protection measures (e.g., Alkhalifah & Alghafis, 2022; Heirman et al., 2013; Ho et al., 2017). However, the impact of subjective norms on protection behaviour has also been shown to vary between genders. For example, Lee and Kozar (2005) found that, compared with the males in their study, females were more influenced by the opinions of their peers when it came to using anti-spyware systems. In addition, Machuletz et al. (2018) found that females used more privacy protection measures than males, although (in contrast to most studies) they also concluded that the opinions of others generally had little impact on the behaviour of their participants.

2.4. Perceived Behavioural Control

Perceived behavioural control refers to the "ease of performing the behaviour" (Ajzen, 1988, 1991), or the extent to which individuals are confident in engaging in a specific behaviour (Ho et al., 2017). Machuletz et al. (2018) and Wang et al. (2016) found perceived behavioural control to be positively linked to behavioural intentions regarding privacy, thus exerting a significant influence on protective behaviour. However, while Bartsch and Dienlin (2016) also identified a positive relationship between OPL and perceived behavioural control, Heirman et al. (2013) concluded that perceived behavioural control had no influence over intention.

TPB has been criticised by a number of scholars for its assumption that actual behaviour is driven by intention. Alhamad and Donyai (2021) and Jokonya (2017) argued that behaviour is influenced by alternative factors, i.e., emotion, desire, and need. In addition, Sussman and Gifford (2019) stated that intention does not necessarily lead to behaviour, as circumstances may prevent individuals from acting (i.e., cost–benefit assessments may outweigh intention), thus resulting in a behavioural paradox. Sniehotta (2009) criticised most TPB studies for generating results based on correlations between variables, rather than experiments. However, the current study assumes that privacy concerns should be considered a factor in PPB, alongside TPB variables.

2.5. Online Privacy Literacy (OPL) and Concerns

OPL consists of understanding the risks of revealing personal information online, which is composed of two types of knowledge: firstly, awareness of risk and, secondly, the ability to implement appropriate protection measures. Trepte et al. (2015) stated that OPL is a "combination of factual or declarative and procedural knowledge about online privacy" (p. 339). Declarative knowledge refers to an individual's awareness of privacy risks and rights, while procedural knowledge determines how users tend to apply protection measures to manage privacy (Trepte et al., 2015). Similarly, Kaya and Yaman (2021) diverged from previous studies in identifying two types of OPL knowledge: firstly, technical expertise and, secondly, social OPL skills (Baruh et al., 2017). In addition, Arachchilage and Love (2014) found that both conceptual and procedural knowledge were statistically significant for enhancing actions taken by online users to prevent threats,

including phishing. This demonstrates that previous findings have shown literate users to combine their awareness of how their personal information is stored, used, or distributed with their personal approach to the kind of personal information they are happy to make public (Wissinger, 2017).

On the other hand, Dinev and Hart (2006b) and Turow and Hennessy (2007) found that OPL negatively impacted PPB due to the OPL hierarchy, i.e., privacy protection measures are generally reduced as OPL reduces privacy concerns. Desimpelaere et al. (2020) identified a paradoxical effect of OPL. Their survey revealed that children with a higher level of literacy reported fewer concerns and intended to disclose more information, while their empirical phase showed that users with higher OPL levels undertook more engagement with PPB. Further research has shown that levels of OPL did not reflect, or only weakly reflected, protection measures, while at the same time having a negative influence on privacy concerns (e.g., Machuletz et al., 2018; Kaya & Yaman, 2021; Sindermann et al., 2021).

The above discussion reveals that increased literacy concerning privacy leads to corresponding increases in privacy-conscious behaviour. This was also anticipated by the current study due to the collective culture of MENA users. Furthermore, it confirms that privacy literacy not only has a direct impact on privacy behaviour, but also exerts an indirect influence through several mediating variables, including (1) attitudes to privacy; (2) subjective norms; (3) perceived behavioural control; (4) intention; and (5) privacy concerns. The present study, therefore, expects the following. Firstly, that higher levels of literacy concerning privacy will encourage privacy protection, leading to more positive subjective norms, and empowering individuals to pursue privacy-conscious behaviour. Secondly, that privacy intentions will form a positive mediator, reflecting proactive commitment to privacy-conscious actions. Finally, that privacy concerns will prove a negative mediator, i.e., an increase in privacy literacy encourages privacy-conscious behaviour. This resulted in the following hypotheses:

H1: *The privacy literacy of users influences their privacy behaviour when using digital media platforms.*

H2: *Privacy attitudes, subjective norms, perceived behavioural control, intention, and concerns mediate the relationship between privacy literacy and privacy behaviour when using digital media platforms.*

Gender differences are an important factor that affects concerns about online privacy. In general, women are more concerned about their privacy and more susceptible to risk (Fogel & Nehmad, 2009). A study by Hoy and Milne (2010) found that, while both men and women were concerned about how their information was used, women were more concerned than men. Likewise, Tufekci (2008) found that males were more open to disclosing their personal information with others. However, Huang et al. (2018) reported contrary results, as men were found to be more concerned about their privacy. Nevertheless, Mutambik et al. (2023) recently argued that privacy concerns differ between gender, age group, and cultural context. This idea is supported by an earlier study by Zhang and Fu (2020), who found that Western people are more concerned about privacy than Asian people. Thus, the present study of MENA users predicted that the relationship between privacy literacy and behaviour would be enhanced by (1) age, (2) being female, and (3) possessing a higher level of education. This resulted in the following hypothesis:

H3: *Users' gender, age, and educational level moderate the relationship between privacy literacy and their privacy behaviour in using digital media platforms.*

The current study, therefore, employed a model guided by TPB, with OPL as an independent variable directly influencing privacy behaviour. In addition, the model contained

five factors acting as moderator variables to mediate the relationship between OPL and PB, as included in H2: (1) privacy concerns; (2) subjective norms; (3) privacy intention; (4) privacy attitudes; and (5) perceived behaviour control. Moreover, H3 examined the moderated variables of gender, age, and educational level. The hypotheses and the relationships between the constructs are summarised in Figure 1.

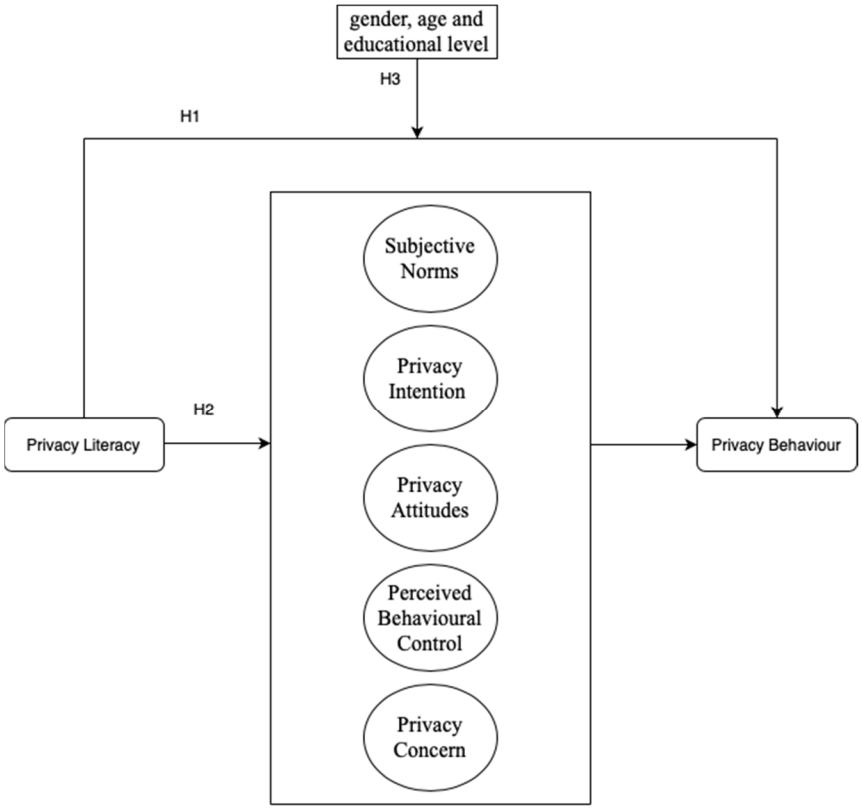

Figure 1. Conceptual model.

3. Methods

This research applied a sequential mixed-method approach to obtain a comprehensive and rigorous undersetting of the phenomena in question (Creswell et al., 2004). It included two sub-studies consisting of an online survey and online self-directed interviews. Thus, the results of both studies, when combined, would allow for a holistic overview of the main research problem to be obtained; while the quantitative study offers generalisable results, the qualitative one provides richer understandings of these findings while also increasing their validity.

Study One consisted of a survey focusing on three issues: (1) whether there is a relationship between OPL level and privacy behaviour; (2) whether differing factors of TPB and privacy concerns mediate the relationship between OPL and privacy behaviour; and (3) whether it is possible to identify the moderating role of demographic factors in these relationships. Study Two undertook an in-depth investigation of the actual practice of online privacy behaviour alongside the reasons for the participants' choices when it came to online privacy protection measures. The data were collected from five countries of the MENA region, which itself contains 19 countries. However, to ensure an effective representation of the sample regarding the entire population of the MENA region with its slight regional differences, as mentioned earlier, the participants were selected from five of the largest countries in the area (i.e., Saudi Arabia, Oman, Egypt, Sudan, and Algeria).

Before undertaking the empirical research phase, the Research Ethics Committee approved the research procedures for the practical stages in accordance with the University Code of Practice. Participants took part in this research voluntarily. In the second study, participants were asked to sign a consent form before the study could begin. In addition, at the end of the study, two participants were provided with an email address they could contact to withdraw from the study. This was if they wished to do so. The interviews were conducted in Arabic because it was the official language of the participants. Afterwards, English translations of the cited materials were conducted.

4. Study One

This cross-sectional study was undertaken with 1040 voluntary participants across the MENA region using a survey created using Google Forms and distributed online through various digital media platforms. It took place over a period of two months, ending in August 2022. The participants were aged between 18 and 65, with half being aged between 36 and 45 (see Table 1). A total of 511 were male (49.1%) and 529 female (50.9%). In addition, their levels of education ranged from basic to graduate studies, with most having studied beyond elementary school but not completed intermediate school or gained a diploma (see Table 2).

Table 1. Participant age groups.

Age Range (Yrs.)	Frequency	Valid Percentage
18–25	98	9.4
26–35	241	23.2
36–45	534	51.3
45–60	146	14.0
61–65	21	2.0
Total	1040	100.0

Table 2. Participants' education levels.

Level	Frequency	Valid Percent
Elementary School	118	11.3
Junior High	222	21.3
High School	287	27.6
Diploma	245	23.6
Bachelor's Degree	124	11.9
Graduate Studies	44	4.2
Total	1040	100.0

The data were collected using several scales adopted from previous studies focusing on Internet privacy, with minor adjustments made to ensure all were appropriate for the context of the current research. In addition, we selected established reliable and valid scales from the literature (see Table 3). The items on all the scales were rated on a 7-point Likert scale (from never to always) and all items were translated into Arabic from the original scales, along with being adapted for an Arabic context. Furthermore, we calculated reliability measures for each scale, which were found to be acceptable (see Table 4). We first asked the participants about their age, gender, educational level, and their most frequently used digital media platform.

Table 3. Description of the seven scales used in this study.

Scale	Description	Example
Subjective norms	These were measured using a nine-item scale developed by Dincelli and Goel (2015) which assesses an individual's perceptions of social pressure from family, friends, and other digital media, as well as their influence on performing behaviour on digital media. The participants were also asked to rate the influence of more specific behaviours, i.e., posting and creating a personal profile.	"My family and/or friends influence the way I use digital media."
Privacy intentions	These were measured using eight items on a scale developed by Dincelli and Goel (2015), then used to assess the participants' intentions to apply privacy protection measures, such as changing passwords, restricting friendships, changing privacy settings, and taking cautious actions to combat security and other violations. The participants were also asked to rate their social privacy intentions.	"I will make an effort to enhance my online security."
Perceived behavioural control	This was measured using a scale of three items proposed by Hong and Thong (2013), which asked the respondents to rate the degree of discomfort experienced from losing control of their personal information, or the way their information could be used or collected.	"I am usually bothered when I do not have control over the personal information that I provide to digital media platforms."
Privacy attitudes	These were measured using three items on a scale proposed by Ho et al. (2017) asking respondents to evaluate their privacy protective behaviours. It was assumed that, when positive ratings were given to a behaviour, there was an increased probability of engaging in this behaviour.	"It is good to engage in privacy protection behaviours on digital media platforms."
Online Privacy Literacy	This was measured using a scale proposed by Bartsch and Dienlin (2016). The scale consists of six items asking about privacy literacy in relation to Facebook, although it can also be adopted to measure the literacy of any other digital media platform. Thus, Kaya and Yaman (2021) adapted Bartsch and Dienlin's (2016) scale to assess privacy literacy on various digital media platforms.	"I know how to delete or deactivate my account."
Privacy concerns	These were measured using a four-item scale employed by Ho et al. (2017) measuring the degree of worry concerning privacy experienced while using digital media.	"How concerned are you about your online personal privacy on digital media?"
Privacy behaviour	This was measured on a scale developed by Dienlin and Trepte (2015), which examined three types of privacy behaviour, i.e., informational, social, and psychological. Each type of privacy was measured by three items asking the respondents to rate how frequently they performed certain behaviours.	"Do you currently restrict access to your digital media account?"

Table 4. Descriptive statistics for variables used to measure participants' privacy.

	Mean	SD	Kurt.	Skew.	Scale Range	α
Subjective Norms	4.22	1.26	−0.365	−0.411	6	0.96
Privacy Intention	4.21	1.22	−0.252	−0.285	6	0.96
Perceived Behavioural Control	4.23	1.22	−0.193	0.076	6	0.90
Privacy Attitudes	4.30	1.24	−0.224	−0.381	6	0.91
Privacy Literacy	3.11	0.78	−0.178	−0.281	4	0.93
Privacy Concern	4.33	1.30	−0.152	−0.361	6	0.95
Privacy Behaviour	3.85	1.25	−0.539	0.317	6	0.95

5. Results

Descriptive Statistics

Before the models were tested, the variables were inspected using descriptive statistics (see Table 4).

This study employed the Hayes Process Macro for SPSS, Model 4, predicating that the users' privacy literacy exerts a direct impact on their behaviour when using digital media platforms. The results revealed a significant total impact, both direct and indirect ($\beta = 1.324$, $p < 0.001$). Furthermore, they highlighted a significant direct impact ($\beta = 0.198$, $p < 0.001$), as well as a marked indirect influence by means of intention ($\beta = 0.192$, $p < 0.01$). In addition, there was a significant indirect effect of privacy literacy on privacy behaviour through privacy concern ($\beta = 0.869$, $p < 0.001$). This indicated that intention and privacy concerns were found to partially mediate the relationship between privacy literacy and behaviour. The positive nature of the direct impact, combined with the positive indirect influences, indicated a complementary mediation outcome. However, the results failed to reveal any further indirect influence of attitudes towards privacy, along with subjective norms and perceived behavioural control. A summary of the mediation variables is presented in Table 5.

Table 5. Direct and indirect effects according to mediation analysis.

	Effect	B	t-Value	sig.	LLCI	UddLCI
Privacy Literacy	Direct	0.198	4.208	<0.001	0.106	0.290
Attitude	Indirect	0.081	1.579	0.115	−0.015	0.134
Subjective Norms	Indirect	−0.049	−1.259	0.209	−0.100	0.022
Perceived Behavioural Control	Indirect	0.034	0.635	0.525	−0.056	0.109
Intention	Indirect	0.192	3.339	<0.01	0.061	0.234
Privacy Concern	Indirect	0.869	20.397	<0.001	0.546	0.662

This study entered the calculated interaction terms into SPSS in order to determine whether age, gender, and education level proved to be moderators of the relationship between privacy literacy and behaviour (H3). This preliminary investigation found significant interactions between privacy literacy and the factors age and level of education, which were consequently entered as moderators into the Hayes Process Macro for SPSS, Model 2, with gender entered into the model as a control variable. The results demonstrated the significant impact of the overall model, which included all variables and interaction terms [$R^2 = 0.69$; $F(6,1033) = 390.645$, $p < 0.001$]. The interaction between age and privacy literacy exerted a significant positive impact on behaviour (R^2 change = 0.001, $\beta = 0.127$, $t = 4.71$, $p < 0.001$). Therefore, age was deemed to act as a significant moderator in strengthening the relationship between privacy literacy and behaviour. On the other hand, the interaction between education and privacy literacy was not identified as being significant ($\beta = 0.027$, $t = 1.21$, $p = 0.226$).

6. Study Two

Study Two measured the participants' caution towards their privacy online in order to answer the research questions about privacy concerns being reflected in privacy protection behaviour. It employed online self-directed interviews to determine the participants' willingness to read both privacy policies and the terms of service before registering for digital media platforms, which also involved providing personal information. According

to Lim (2002), this type of interview involves confronting participants with a screen record of their actual online behaviour and requesting that they reveal their thoughts and feelings.

At the end of Study One, the participants were asked to tick a box and provide their email to indicate that they were willing to take part in the subsequent interviews. Ninety-five volunteered, aged between 18 and 49 (M = 21, SD = 4.74), 78% of whom were female and 22% male. The data collection period for Study Two took place over a period two months, starting on 22 November 2022.

7. Procedure

Following the results of Study One, an invitation was also sent through the same digital media platforms to invite participants to take part in an online interview regarding a proposed digital media platform which, they were told, the researchers aimed to launch in the near future. After each participant signed an informed consent form and approval had been granted by the ethics committee at the authors' university, the interviews (each lasting approximately 15 min) were conducted and recorded on the Zoom platform. At the beginning of the interview, the participants were asked to click on a link to a digital media platform named Twassul (an Arabic word meaning communication) and assess whether they were willing to register. The participants were informed that they could take as long as they wished to scrolling through the website.

As shown in Figure 2, the website's front page imitated the interfaces of well-known digital media platforms, i.e., Facebook and Twitter. It asked the participants to fill in their names, email, gender, and date of birth. To verify the participants' responses in Study One, the researchers selected one item from each of the seven scales applied in the survey, which were added to registration page forms as optional privacy settings. The participants were asked to indicate whether or not they agreed with seven options regarding the privacy of their account: (1) to share posts only with those they added as friends; (2) to show personal data to everyone; (3) to receive a reminder to change their password every six months; (4) to receive reminders to change and review privacy settings every six months; (5) to allow access to their account from Google; (6) to allow others to add them without notification; and (7) to receive an alert email when someone logged into their account.

Figure 2. Twassul interface.

Before clicking on the icon allowing them to register, the participants were asked to tick two mandatory boxes to indicate that they agreed with the privacy policy and terms of service of the platform, as required by almost all well-known digital media platforms. In addition, they were able to click on the policy or the terms, enabling pop-up pages to appear with the appropriate content. Both the privacy policy and the terms of service pages imitated, with only a few modifications, similar pages on Facebook regarding the length and content of the terms and conditions. The clicks on these pages, along with and the amount of time spent on each page, were measured to establish the number of participants who read the terms and conditions. In addition, unacceptable privacy violation conditions were included on the page to measure whether they were read by the participants. The following were indicated as being low, medium, and high privacy violation conditions:

1. By using Twassul, you agree that we may use and sell your personal data to advertisers and share information that directly identifies you (such as your name, age, geographic location, photograph, email address, or other contact information) or allow any third party to use such information in any way they deem to serve their interests, even if it may cause you direct or indirect physical or mental harm.
2. By using Twassul, you agree that we may apply on your behalf to withdraw from your university studies if you are a student, or to resign from your job if you are an employee, at any time and without giving reasons. If one of these two cases does not apply to you at the present time, this permission continues until 2040.
3. By using Twassul products covered by these terms, you agree that we can, at any time, exploit your credit card stored in your account on the Twassul website and use it in any way we see fit. If you do not have a credit card, you agree to grant us access to your bank accounts at any time, without the need to provide any justification.

For this research, we observed the participants throughout the registration process. Once they clicked on the 'register' symbol, a message appeared stating that the site was an experiment, as part of a research project measuring awareness of privacy policies, and, therefore, was not a real digital media site. If the participants wished to obtain additional information, they were encouraged to click on a link that provided details about the research. If they did not want to share the data they had entered, they were asked to send an email to a given email address to enable their information to be permanently cancelled and not viewed by the researchers. After this stage was completed, we conducted semi-structured interviews, in which the participants were questioned about their experience of completing the registration process in Study Two. The aim of the study was then revealed to the participants in order to double-check that they were willing to have their data collected. In addition, we applied thematic analysis to the interviews using an inductive approach, following Creswell's (2014) six-step method, and using MAXQDA 12.

8. Results

The data analysis of both the registration forms on Twassul and the self-confrontation interviews revealed the following results. Firstly, the majority of the participants revealed personal information when registering for Twassul, i.e., their real names and email addresses. However, a small number of the female volunteers provided only part of their name, replacing their last name (i.e., family name) with their father's name. They explained that concealing their last names gave them more freedom and kept their activities private from their friends and relatives. In addition to these factors relating to privacy protection, phone numbers were used differently by the male and female participants during the registration process, with 72% of the females using their phone numbers to register due to considering it easier than writing their email addresses and being more accessible. However, none of the male participants registered using their phone numbers. It was notable

that the participants did not classify their dates of birth, gender, and levels of education as sensitive information, and were willing to share such details. It was also significant that the participants commented during the interviews that they did not feel any shame about revealing their ages due to the fact that they were still young.

When it came to the optional privacy settings on the registration page, the first and last were the most frequently selected by both male and female participants. The first optional privacy setting concerned sharing posts with app users, asking participants if they preferred to "share posts only with people added as friends". However, in the interviews, the participants commented that they preferred to restrict posts to friends, particularly in relation to photographs. The last optional privacy setting statement concerned core OP protection, asking whether the participants wished to receive an alert email whenever a login was made to their account. The majority agreed that, even if they did not select it, this protection measure was beneficial. The least frequently selected privacy setting by both the male and female participants was "Allow others to add you without notifying". In the interviews, the participants indicated that they preferred to review friendship requests before accepting them. Moreover, the least frequently selected optional privacy setting by the female participants was to display personal data to everyone.

In the interviews, a little over one-third of both female and male participants indicated that they were concerned about online privacy settings. However, they did not consider it practical to change their passwords and privacy settings every six months, and the inconvenience of receiving these emails was the main reason most gave, preferring to reduce the number of emails they received. Similarly, they stated that they did not wish to change their privacy settings on a social media app, as this becomes mor problematic after a user becomes active, with one participant stating "I would not change my privacy settings even if I was aware that the app had updated the privacy policy to something that could harm my privacy". In addition, the participants who did not selected the privacy option given in Google searches were concerned that the research results could appear with their photographs and posts (see Table 6).

Table 6. Optional online privacy settings.

Gender	OPS1	OPS2	OPS3	OPS4	OPS5	OPS6	OPS7
Female	72%	25%	46%	46%	40%	28%	71%
Male	85%	40%	40%	50%	40%	30%	80%

The results showed that, while one-third of the male participants clicked on the privacy policy's and terms and conditions, only a small number of females did the same (Table 7). However, the results showed that the average amount of time spent by the participants reading the terms and conditions was less than one minute, indicating that none examined them in detail (Table 8). In addition, the longest amount of time spent was less than two minutes, i.e., the participants only scanned the page. Nonetheless, three participants refused to register after observing the violation conditions while reading the privacy policy and terms and conditions. They stated in their interviews that they were always cautious due to being aware of the risk of becoming victims of online privacy policies.

Table 7. Participants who clicked on the privacy policy and terms and conditions.

Gender	% Who Clicked on Privacy Policy	% Who Clicked on Terms and Conditions
Female	3%	6%
Male	30%	30%

Table 8. Time spent reading about the registration process.

Gender	Time (Seconds) on Privacy Policy	Time (Seconds) on Terms and Conditions	Registration Time
Female	24	47.5	98
Male	33	41	118.5

During the interviews, the participants highlighted several reasons for failing to read the privacy policy and the terms and conditions. The majority stated that privacy policies tend to be long and tedious and were generally similar on most websites and apps. They also mentioned the issue of trust, both in the researcher who had developed the Twassul website, and in social platforms and websites in general. In addition, the participants also noted that they considered the government would deactivate any unreliable platform. However, their main reason for trusting the platform and websites was not having previously experienced the implications of such risks, while noting that they felt platforms tended to be manipulative and would always find ways of using their information. Thus, one participant stated "They will use our information either way". By contrast, several participants stated that there was no reason for a platform with several millions of users to track each one, or to use their personal information.

9. Discussion and Conclusions

The results of the current study revealed several important results contributing to the field of privacy. One of the most interesting findings is that Study One found that OPL is related to PPB. This supports previous studies by Afif et al. (2023), Baruh et al. (2017), Desimpelaere et al. (2020), Lund and Agbaji (2023), and Masur (2020). On the other hand, Study Two revealed that, even though most of the participants were cautious about the OPS they selected, a number of inconsistencies in PPB were highlighted by their actions towards the privacy policy and terms of use.

When it came to the factors potentially mediating this association, most of the findings derived from both analytical procedures in Study One corroborating each other, as well as the significance of the mediators and associated paths. This research, therefore, found that intention, privacy concerns, and attitudes positively mediated the relationship between privacy literacy and behaviour. Furthermore, this confirmation of a relationship between intention and PPB is consistent with the conclusions of Ajzen and Fishbein (1980), Dinev and Hart (2006a), and Baruh et al. (2017). Likewise, the mediating role of privacy concern identified in this study partially matches previous research determining a positive effect of privacy concerns on behaviour (e.g., Baruh et al., 2017). In addition, previous research, including that of Ho et al. (2017) and Machuletz et al. (2018), revealed that positive attitudes were also linked to engagement behaviour. However, perceived behavioural control and subjective norms were found to exert no significant indirect influence on privacy behaviour in this study, which contrasts with the findings of Heirman et al. (2013) and Ho et al. (2017), who reported social factors as having the greatest influence on PPB. This result is particularly unexpected, given the nature of MENA societies and the role played by norms.

The results of Study One utilising the Hayes' PROCESS macro showed that age exerted a significant positive impact on privacy behaviour. Moreover, this led to a more nuanced understanding of their relationships, albeit at the expense of their individual explanatory capacity. This result is in line with several previous studies revealing age as a positive moderator of the relationship between OPL and PPB (e.g., Desimpelaere et al., 2020; Sindermann et al., 2021).

In addition, the findings of Study One also revealed that gender had no significant influence on the association between OPL and PPB. Such a result was unexpected for the

MENA region due to the general assumption that its female population tends to be highly conservative and might exhibit heightened privacy concerns due to the cultural norms of Islamic society (Park, 2013; Sindermann et al., 2021; Kaya & Yaman, 2021). Interestingly, Study Two offered a contrary perspective, in that male participants demonstrated more engagement with privacy protection. In particular, males spent more time registering for the website and reviewing the privacy policies. A third of the males clicked on the privacy policy and terms of use to check the details. In addition, there were more males who selected the optional privacy setting than females. This result is in accordance with the findings reported by Huang et al. (2018). Generally, the males' protective behaviour could be explained by their desire for a sense of control over online activities.

This research has several implications. Firstly, it indicates that users are able to make better judgements about their online choices when they understand the relationship between OPL and privacy protection. Secondly, it emphasises the necessity of educational programmes to raise awareness of Internet privacy. Finally, it can serve as a road map for developers to build user-friendly interfaces enabling users to make informed decisions concerning their online privacy.

However, it should be noted that, due to the current research being conducted in the MENA region, it will be vital to use caution in generalising the results to other populations. Thus, future research could adapt the sequential mixed-methods approach to study OPL and behaviour in other nations or regions, followed by comparing the findings with those of the current study. In addition, future studies could broaden the range of factors examined, including those that have not been considered in the current research, and which may act as mediators of the relationship between users' privacy literacy and their privacy behaviour. Finally, this research recommends that future studies could test the privacy protection behaviours of the three theorised groups, which may yield interesting findings and could lead to the development of a typology of user behaviours and potentially draw up a framework for user education and privacy protection.

Author Contributions: All authors of this article made equal contributions to its development. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Deanship for Scientific Research at King Abdulaziz University for funding this research under Grant No. PH: 002-848-1443.

Institutional Review Board Statement: Ethical approval was obtained from the Ethics Committee in the Faculty of Media and Communication at King Abdulaziz University, which approved the research procedures in accordance with the University Code of Practice.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are available on request due to restrictions of privacy.

Conflicts of Interest: The authors report no conflicts of interest.

References

Abokhodair, N., & Vieweg, S. (2016, June 4–8). *Privacy & social media in the context of the Arab Gulf*. DIS 2016 Conference on Designing Interactive Systems: Fuse (pp. 672–683), Brisbane, Australia. [CrossRef]

Afif, N. S., Basa, M., & Zakharia, A. (2023). Analysis of digital literacy in the use of the internet in students. *Jurnal Scientia*, *12*(03), 2714–2718. Available online: http://infor.seaninstitute.org/index.php (accessed on 27 December 2024).

Ajzen, I. (1988). *Attitudes, personality, and behavior*. Open University Press.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. [CrossRef]

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice-Hall.

Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A conceptual model for investigating the effect of privacy concerns on e-commerce adoption: A study on United Arab Emirates consumers. *Electronics*, *11*(22), 3648. [CrossRef]

Alhamad, H., & Donyai, P. (2021). The validity of the theory of planned behaviour for understanding people's beliefs and intentions toward reusing medicines. *Pharmacy*, *9*(1), 58. [CrossRef]

Alkhalifah, A., & Alghafis, A. (2022). The effect of privacy concerns on childern's behavior on the internet: An empirical study from the parents'. *Journal of Management Information and Decision Sciences*, *25*(1), 1–24.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. [CrossRef]

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154. [CrossRef]

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. [CrossRef]

Cho, H., Metzger, M., Trepte, S., & Nekmat, E. (2023). A cross-country study of comparative optimism about privacy risks on social media. *International Journal of Communication*, *17*, 2003–2023.

Colnago, J., Cranor, L., & Acquisti, A. (2023). Is there a reverse privacy paradox? An exploratory analysis of gaps between privacy perspectives and privacy-seeking behaviors. *Proceedings on Privacy Enhancing Technologies*, *2023*(1), 455–476. [CrossRef]

Creswell, J. (2014). *Research design* (4th ed.). SAGE.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2004). Advanced mixed methods research designs. In A. Tashakkori, & C. Teddlie (Eds.), *Handbook of mixed methods in social & behavioral research* (pp. 209–240). SAGE Publications.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. [CrossRef]

Dennis, E., Martin, J., Lance, E., & Hassan, F. (2019). Media use in the Middle East: A seven-nation survey. *Biometric Technology Today*, *11*(10), 8–11. [CrossRef]

Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in Human Behavior*, *110*, 106382. [CrossRef]

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. [CrossRef]

Dincelli, E., & Goel, S. (2015,). *Research design for study of cultural and societal influence on online privacy behavior*. 2015 IPIP 8.11/11.13 Dewald Roode Information Security Research Workshop, Newark, DE, USA.

Dinev, T., & Hart, P. (2006a). Privacy concerns and levels of information exchange: An empirical investigation of intended e-services use. *E-Service Journal*, *4*(3), 25. [CrossRef]

Dinev, T., & Hart, P. (2006b). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. [CrossRef]

Farooq, A., Salminen, J., Martin, J., Aldous, K., Jung, S. G., & Jansen, B. J. (2024). Exploring social media privacy concerns: A comprehensive survey study across 16 Middle Eastern and North African countries. *IEEE Access*, *12*, 147087–147105. [CrossRef]

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. [CrossRef]

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *16*(2), 81–87. [CrossRef] [PubMed]

Ho, S. S., Lwin, M. O., Yee, A. Z. H., & Lee, E. W. J. (2017). Understanding factors associated with Singaporean adolescents' intention to adopt privacy protection behavior using an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 572–579. [CrossRef] [PubMed]

Hofstede, G. (2011). Dimensionalizing cultures. *Online Readings in Psychology and Culture*, *2*(1), 1–26. [CrossRef]

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly: Management Information Systems*, *37*(1), 275–298. [CrossRef]

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, *10*(2), 28–45. [CrossRef]

Huang, J., Kumar, S., & Hu, C. (2018). Gender differences in motivations for identity reconstruction on social network sites. *International Journal of Human-Computer Interaction*, *34*(7), 591–602. [CrossRef]

Jokonya, O. (2017, April 23). *Critical literature review of theory of planned behavior in the information systems research*. DEStech Transactions on Computer Science and Engineering, AMEIT (pp. 177–181), Shanghai, China. [CrossRef]

Kaya, S., & Yaman, D. (2021). Examining University students' online privacy literacy levels on social networking sites. *Participatory Educational Research*, *9*(3), 22–45. [CrossRef]

Lee, B. Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, *48*(8), 72–77.

Lei, K., Fang, J., Zhang, Q., & Yang, X. (2020). Blockchain-based cache poisoning security protection and privacy-aware access control in NDN vehicular edge computing networks. *Journal of Grid Computing*, *18*(4), 593–613. [CrossRef]

Li, Y., Huang, Z., Wu, Y. J., & Wang, Z. (2019). Exploring how personality affects privacy control behavior on social networking sites. *Frontiers in Psychology*, *10*, 1–9. [CrossRef] [PubMed]

Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *23*(5), 675–694. [CrossRef]

Lund, B., & Agbaji, D. (2023). Information literacy, data literacy, privacy literacy, and ChatGpt: Technology literacies align with perspectives on emerging technology adoption within communities. *Human Technology*, *19*(2), 163–177. [CrossRef]

Machuletz, D., Laube, S., & Böhme, R. (2018, April 21–26). *Webcam covering as planned behavior*. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1–12). [CrossRef]

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. *Media and Communication*, *8*(2), 258–269. [CrossRef]

Masur, P. K., Epstein, D., Quinn, K., Wilhelm, C., Baruh, L., & Lutz, C. (2023). Comparative Privacy Research: Literature Review, Framework, and Research Agenda. *SocArXiv*. [CrossRef]

Mutambik, I., Lee, J., Almuqrin, A., Zhang, J. Z., Baihan, M., & Alkhanifer, A. (2023). Privacy concerns in social commerce: The impact of gender. *Sustainability*, *15*(17), 12771. [CrossRef]

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. [CrossRef]

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, *40*(2), 215–236. [CrossRef]

Petronio, S., & Altman, I. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press. [CrossRef]

Rassed. (2014). *The attitude of online users in the MENA region to cybersafety, security and data privacy*. Ministry of Information and Communications Technology.

Sabbah, K., & Sabbah, Y. (2023). Digital literacy in the palestinian public schools: The influence of gamification-based learning. In *Lecture notes in educational technology* (Vol. 2023, pp. 61–79). Springer. [CrossRef]

Sadaf, A., & Gezer, T. (2020). Exploring factors that influence teachers' intentions to integrate digital literacy using the decomposed theory of planned behavior. *Journal of Digital Learning in Teacher Education*, *36*(2), 124–145. [CrossRef]

Sadaf, A., & Johnson, B. L. (2017). Teachers' Beliefs About Integrating Digital Literacy Into Classroom Practice: An Investigation Based on the Theory of Planned Behavior. *Journal of Digital Learning in Teacher Education*, *33*(4), 129–137. [CrossRef]

Schäwel, J. (2018). *How to raise users' awareness of online privacy [der Universität Duisburg-Essen]*. Duidburg-Essen Publication. [CrossRef]

Sindermann, C., Schmitt, H. S., Kargl, F., Herbert, C., & Montag, C. (2021). Online Privacy Literacy and Online Privacy Behavior–The Role of Crystallized Intelligence and Personality. *International Journal of Human-Computer Interaction*, *37*(15), 1455–1466. [CrossRef]

Sniehotta, F. (2009). An Experimental Test of the Theory of Planned Behavior. *Applied Psychology: Health and Well-Being*, *1*(2), 257–270. [CrossRef]

Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October 14–17). *E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior*. EC '01: 3rd ACM Conference on Electronic Commerce (pp. 38–47), Tampa, FL, USA. [CrossRef]

Sussman, R., & Gifford, R. (2019). Causality in the Theory of Planned Behavior. *Personality and Social Psychology Bulletin*, *45*(6), 920–933. [CrossRef] [PubMed]

Trepte, S., Reinecke, L., Ellison, N. B., Quiring, O., Yao, M. Z., & Ziegele, M. (2017). A Cross-Cultural Perspective on the Privacy Calculus. *Social Media and Society*, *3*(1), 1–13. [CrossRef]

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In *Reforming European data protection law* (Vol. 20, pp. 333–365). Springer. [CrossRef]

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *New Media and Society*, *20*(1), 141–161. [CrossRef]

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36. [CrossRef]

Turow, J., & Hennessy, M. (2007). Internet privacy and institutional trust: Insights from a national survey. *New Media and Society*, *9*(2), 300–318. [CrossRef]

Uzun, A. M., & Kilis, S. (2020). Investigating antecedents of plagiarism using extended theory of planned behavior. *Computers and Education*, *144*(September), 103700. [CrossRef]

Vannucci, A., Simpson, E. G., Gagnon, S., & Ohannessian, C. M. C. (2020). Social media use and risky behaviors in adolescents: A meta-analysis. *Journal of Adolescence*, *79*, 258–274. [CrossRef]

Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International Journal of Information Management*, *36*(4), 531–542. [CrossRef]

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy*, *11*(2), 378–389. [CrossRef]

Zeng, F., Ye, Q., Li, J., & Yang, Z. (2021). Does self-disclosure matter? A dynamic two-stage perspective for the personalization-privacy paradox. *Journal of Business Research*, *124*, 667–675. [CrossRef]

Zhang, R., & Fu, J. S. (2020). Privacy management and self-disclosure on social network sites: The moderating effects of stress and gender. *Journal of Computer-Mediated Communication*, *25*(3), 236–251. [CrossRef]