Communication Reports
Vol. 00, No. 00, 2024, pp. 1–21

The Costs of Connectivity: WhatsApp Usage, Privacy Concerns, and Protection Behaviors in Israel

Yaron Ariel & Eilat Chen Levy

This study examines the implications of WhatsApp usage in Israel, focusing on the interplay between usage patterns, privacy concerns, and protection behaviors. Using a sample of 505 participants, this study aimed to understand whether users are aware of privacy issues and how this awareness translates into proactive protection actions. Results showed a significant positive correlation between usage frequency and privacy concerns, but no significant correlation between usage frequency and protection behaviors. However, there was a strong positive correlation between privacy concerns and protection behaviors, with privacy concerns mediating the relationship between usage and protection behaviors. This study underscores the importance of understanding user behavior and privacy perceptions, providing insights for future research and policymaking to enhance privacy on digital platforms.

Keywords: privacy concerns; privacy paradox; privacy protection behaviors;; WhatsApp

Introduction

Since its inception in 2009, WhatsApp, a leading messaging application owned by Meta since 2014, has experienced rapid growth worldwide (Awwad, 2021; Wijnberg

Correspondence to: Yaron Ariel, Department of Communication, Max Stern Yezreel Valley College, Tel Adahim 1930600, Israel E-mail:yarona@yvc.ac.il
Yaron Ariel (Ph.D., University of Haifa) is a full-time faculty member at the Communication Department of Yezreel Valley College, Israel. His expertise includes computer-mediated communication, political communication, online interruptions, and social networks. http://yaronariel.com Eilat Chen Levy (Ph.D., University of Haifa) is a researcher at the Department of Communication at the College of Jezreel Valley, Israel. Her research interests include online interruptions, mobile phones, computer-mediated communication, Wiki systems for learning, and simulation games

ISSN 0893-4215 (print)/ISSN 1745-1043 (online) © 2024 Western States Communication Association
DOI: 10.1080/08934215.2024.2424552

& Le-Khac, 2021), with approximately 3 billion unique active users worldwide, WhatsApp is the most popular instant messaging platform (Ceci, 2023). WhatsApp has achieved extensive penetration in Israel, with an estimated 90% of the population utilizing it. This widespread adoption has led to its integration into various aspects of society, including organizations, educational institutions, and families (Wiener & Stegman, 2023). The platform functions extensively as a way to maintain connections with friends and family with an overwhelming majority of users (Kemp, 2023). The popularity of WhatsApp in Israel can be attributed to its user-friendly format and widespread acceptance, especially during times of crisis or conflict (Avidar et al., 2017).

WhatsApp rapid rise to ubiquity has not been free of controversy, as the platform has frequently found itself at the epicenter of debates regarding data privacy (Farooq et al., 2024; Mols & Pridmore, 2021). WhatsApp's success can partly be attributed to its strategic utilization of the widespread availability of standard mobile devices. By leveraging this ubiquity, the platform offers diverse communication modes, including text messages, voice files, documents, and videos. This multimodal communication capability has positioned WhatsApp as an indispensable conduit for international interactions (Kustijono & Zuhri, 2018).

Sundaram and Shetty (2022) maintained that privacy efficacy, compounded by alterations triggered by COVID-19, escalated individuals' need to proactively safeguard their data and devices. Moreover, they identified a positive association between an organization's choice of software and privacy concerns, albeit without a substantial impact on protective behaviors. Indeed, the onset of the COVID-19 pandemic has significantly amplified the role of WhatsApp in our daily lives (Tunjera, 2023). As the world grappled with lockdowns and social distancing, the need for reliable communication channels, efficient information exchanges, and accessible entertainment has become more pronounced. Consequently, WhatsApp has experienced a substantial increase in usage, a surge particularly evident in COVID-19-related discussions, educational content dissemination, and official news distribution (Tan et al., 2021). These trends underscored WhatsApp's ability to adapt and respond to the evolving global needs during crises. The platform demonstrated its capacity to serve as a critical tool for information dissemination, helping bridge the gap between individuals and institutions during unprecedented social isolation.

Moreover, as Aizenkot and Kashy-Rosenbaum (2018) and Ahad and Lim (2014) suggest, WhatsApp's strengths extend beyond crisis communication. The platform caters to various user needs and permeates various aspects of life. It is a personal communication medium, facilitator of professional collaborations, and catalyst for civic activism. The app has become a go-to platform for individuals to stay connected with friends and family, share experiences, and maintain social ties despite physical distance. In the professional sphere, collaboration is fostered by providing a platform for real-time communication, document sharing, and group discussions. In the context of civic activism, it empowers communities by providing a platform for mobilization, information sharing, and collective action.

The key attributes of WhatsApp, such as replicability and scalability, augment its usability, enabling seamless content dissemination independent of the original context or the sender. The platform adopted end-to-end encryption in 2016, despite igniting privacy and security debates (Santos & Faure, 2018), and bolstered user trust by ensuring confidentiality. WhatsApp's unique potential to offer refuge from state surveillance (Johns & Cheong, 2021), thus reducing the cost of political activism (Treré, 2018), has positioned it as a more favorable option than less private social media platforms such as Facebook and Twitter. This is further reinforced by the collapse of context on such platforms (Brandtzaeg & Lüders, 2018).

WhatsApp and Privacy

Despite the platform's data protection settings, WhatsApp's privacy policies have become contentious due to user and contact data collection and sharing. This controversy has fostered the perception of WhatsApp as a risk to data protection, as highlighted by the numerous press reports and online resources that underscore its security shortcomings. Various studies have explored multiple aspects of WhatsApp's privacy policy and its implications for users. Some studies (e.g., Griggio et al., 2021) have focused on the financial exploitation of user data and commodities within WhatsApp's privacy policies. In contrast, others have analyzed governments' awareness and acceptance of privacy policy changes. Ongoing discussions surrounding end-to-end encryption, national security, and privacy conflicts have garnered attention (Olaniyi & Omubo, 2023).

Rastogi and Hendler (2017) critically analyzed the security architecture of WhatsApp messaging platforms, with a specific focus on privacy preservation mechanisms. The authors argued that while encrypting the end-to-end channel was crucial, it was insufficient to protect privacy, as metadata could potentially show connections between individuals, their behavioral patterns, and personal information. Schnitzler et al. (2022) showed that delivery status notifications, a standard feature of mobile instant messengers such as WhatsApp, could unintentionally create a timing-side channel with privacy implications concerning user location. Finally, Liu et al. (2022) addressed the challenge of combating the viral spread of misinformation within encrypted messaging systems, such as WhatsApp, emphasizing the need for effective measures without compromising user privacy. These and other studies have highlighted WhatsApp's privacy concerns and the importance of developing robust privacy-preserving mechanisms.

According to Rastogi and Hendler (2017), WhatsApp architecture is exposed to global surveillance and unauthorized access to user conversations. While it ensures the encryption of communication channels and user data in motion, the company maintains specific metadata, such as delivery time, phone numbers, and content size, which raises privacy concerns. Users were also prompted to share their contact lists.

Finally, WhatsApp stores smartphone metadata on its servers, including phone numbers, timestamps, connection details, and locations, potentially enabling profiling and inference.

Another concern is that Facebook owns WhatsApp and metadata can be leveraged for user profiling and targeted advertising. In 2016, WhatsApp revised its privacy terms to allow the transfer of user data to Facebook. This enabled WhatsApp account information to be used for targeted advertising and marketing messages. Phone numbers serve as unique identifiers, link various personal data sources, and help create comprehensive user profiles (Fiesler & Hallinan, 2018). Thus, while WhatsApp's implementation of end-to-end encryption is a positive step for privacy, concerns persist about storing unencrypted metadata and sharing data with Facebook (Talwar et al., 2022).

Griggio et al. (2022) delved into users' experiences transitioning away from WhatsApp following the 2021 privacy policy update. This study surveyed WhatsApp users from various countries and unearthed intriguing insights into their experiences and obstacles when transitioning to alternative messaging applications. Their study highlighted the potential of messaging interoperability to mitigate the challenges associated with platform switching, with significant implications for human–computer interaction (HCI) research and competition regulation within digital services. While most participants were aware of WhatsApp's privacy policy changes, a third had not read them. The researchers also found that a quarter of the users wanted to migrate away from WhatsApp, yet only a fraction of them succeeded.

This finding underscores the lack of competition in digital markets and its detrimental effects on consumer choices and controls. Users face numerous challenges when transitioning from WhatsApp to other platforms, including network effects, communication functionality, privacy and security, and communication between locations (Dahabiyeh et al., 2023).

Farooq et al. (2024) examined the factors influencing WhatsApp users' intentions to drop out of a platform because of privacy policy changes. They illuminated the catalysts and deterrents of discontinuation, providing valuable insights for both users and the platform by finding that distrust, negative word-of-mouth, and perceived privacy invasion significantly influence users' intentions to drop WhatsApp. Additionally, their research revealed that structural assurance moderated the relationship between distrust and discontinuation intention, suggesting that bolstering structural assurance could dampen the negative effect of distrust on discontinuation intention.

Daradkeh (2023) explored the relationship between social media privacy policies and self-disclosure behavior, revealing that individuals consider privacy policies, trustworthiness, and potential privacy costs when choosing a social media platform and determining their information disclosure level. This aligns with the findings of Chen and Peng (2023), who emphasized the role of perceived affordances, including privacy, in shaping social media use motives and platform selection. They found that users who valued privacy were likely to select platforms that provided robust privacy affordances, thus allowing them to control the visibility of their information and communication. Similarly, Singh and Mishra (2020) highlight that users' decisions to disclose information are influenced by the platform's reputation and perceived control over their data.

Despite privacy concerns, users may continue to use a platform owing to network effects, where the platform's value increases with the number of users, as noted by Griggio et al. (2021). These dynamics suggest that understanding platform choice requires considering both individual privacy concerns and broader social influences, as users navigate their privacy behaviors within the constraints and affordances of different platforms. This connection underscores the importance of privacy as a determinant in the selection and use of social media platforms.

Mars et al. (2019) reviewed WhatsApp guidelines in clinical practice, focusing on the legal, regulatory, and ethical concerns associated with utilizing the platform for sharing sensitive patient information among healthcare professionals. This study aimed to provide insights into the potential development of comprehensive policies for instant messaging in healthcare settings. The authors examined the importance of confidentiality and privacy considerations when using WhatsApp. They discussed preventive measures such as removing individuals from WhatsApp groups to ensure privacy. The main finding of the literature review was that, while healthcare professionals often choose to use instant messaging applications such as WhatsApp because of their simplicity, timeliness, and cost-effectiveness, there needs to be more proper guidelines specifically tailored to their use in healthcare delivery.

Privacy Concerns and Privacy Calculus

Theoretically, the definition of privacy is fundamental for understanding this paradox. Privacy is a fundamental human right that refers to an individual's voluntary and temporary withdrawal from society through physical or psychological means necessary for personal care, intimacy, and communication (Westin, 1967). It can be divided into vertical and horizontal levels, capturing privacy from authorities, institutions, and companies and privacy from peers and other individuals (Masur, 2018). Privacy concerns represent how much individuals care about being able to voluntarily withdraw from other people or societal institutions on the internet, accompanied by an uneasy feeling that their privacy might be threatened.

Privacy concerns form an integral part of privacy calculus. This concept suggests that the decision to share personal information online is influenced by the balance between perceived costs and anticipated benefits (Culnan & Armstrong, 1999). The privacy calculus model assumes that individuals disclose personal information based on a cost-benefit analysis in which the benefits of disclosure are weighed against the associated risks (Dinev & Hart, 2006). The model further postulates that individuals are rational actors who make decisions based on self-interest. They are not driven by altruism and choose not to disclose personal information, unless they perceive personal benefits. Another assumption undergirding this model is that individuals possess complete information regarding the risks and rewards of disclosing personal data and are capable of making informed decisions. However, in practical scenarios, individuals often work with limited information, potentially hindering their ability to accurately gauge the risks and benefits of sharing personal details (Guo et al., 2020; Kordzadeh et al., 2016).

Tang et al. (2021) found that privacy fatigue and concerns significantly influence app users' willingness to disclose personal information, with privacy fatigue having a greater impact. The study introduces privacy fatigue as a new concept and contrasts it with traditional privacy concerns. It also highlights that personality traits like neuroticism, agreeableness, and extraversion affect privacy fatigue and concerns, influencing users' intentions to share information.

Online information sharing refers to the amount of person-related information individuals share when they use the internet and is a more specific concept than communication or self-disclosure, addressing only person-related information such as age, sex, name, address, health, and finances (Dienlin & Trepte, 2015). Many factors influence information sharing, including subjective norms and expected benefits, and often override privacy concerns (Heirman et al., 2013).

Stevic et al. (2022) found a correlation between mobile social media privacy concerns and elevated perceived stress. Notably, this correlation seems unidirectional and lacks the evidence of a reciprocal relationship. The researchers highlighted the negative impact of privacy concerns on individuals' willingness to share their personal information. They argued that enhancing transparency and fair use could bolster individuals' confidence in disclosing such information. It also points out that various factors influence privacy concerns, including personality traits, demographic variables, and experiences. This study emphasizes the significance of addressing privacy issues and fostering transparency and fair use to boost confidence in sharing personal information on mobile social media platforms.

Additionally, others often share personal information, a phenomenon known as "networked privacy," which reduces individuals' power to control the amount of personal information found online (Marwick & Boyd, 2014).

The Privacy Paradox

The privacy paradox has become a growing issue as individuals desire online privacy while simultaneously disclosing significant amounts of personal information online, potentially leading to risks such as identity theft, data breaches, and privacy violations (Acquisti & Grossklags, 2003). This phenomenon has been extensively discussed in the popular media, academic literature, and online forums. However, despite many empirical studies, the underlying reasons for this privacy paradox remain poorly understood.

One of the significant challenges in understanding this paradox is that empirical studies have mainly used a *between*-person perspective to explore the relationship between privacy concerns and online behavior (Baruh et al., 2017; Yu et al., 2020). Empirical studies rarely use *within*-person designs, which is a significant limitation in making causal claims about the relationship between privacy concerns and information-sharing. However, a causal perspective is essential for understanding the privacy paradox, as individuals who become more concerned about privacy should share less personal information online (Dienlin & Trepte, 2015). Thus, conducting studies using within-person designs is necessary to understand the causal relationship between privacy concerns and information-sharing.

Massara et al. (2021) examined the privacy paradox by utilizing a range of mediating variables that impact the relationship between privacy concerns and disclosure behavior. These variables included mental accounting for risks, benefits, and familiarity. The authors discovered that factors such as perceived immediate benefits and familiarity with the data collector could increase disclosure even given privacy concerns. Furthermore, their research emphasized the privacy calculus model and underscored the pivotal role of benefit evaluations in privacy decision-making.

Despite numerous empirical studies on the privacy paradox, the findings remain inconsistent. Some studies have found significant relationships between privacy concerns and information sharing (Dienlin & Trepte, 2015; Heirman et al., 2013; Walrave et al., 2012), whereas others have found no significant relationship (Taddicken, 2014; Tufekci, 2008). A meta-analysis of 37 studies found a small but statistically significant relationship between privacy concerns and online information sharing (Baruh et al., 2017). Dienlin et al. (2023) found that individuals do not significantly alter their online sharing behaviors over time. Therefore, privacy concerns do not have a lasting impact on how much personal information people share online. However, the limited use of within-person designs in these studies remains a significant limitation in making causal claims regarding the relationship between privacy concerns and information-sharing.

The Current Study

This study aimed to comprehensively explore the dynamics of WhatsApp usage in Israel, with a particular focus on privacy concerns and protection behaviors among users. We seek to understand the extent to which frequent WhatsApp users are aware of and concerned about their privacy, and how this awareness translates into proactive privacy protection actions.

Previous research has extensively examined digital communication and privacy concerns; however, a significant gap exists in the understanding of how these concerns manifest in daily high-frequency use scenarios. The widespread reliance on communication has distinct privacy implications for sporadic platform use. This study addresses this gap by analyzing the relationship between the frequency of WhatsApp usage, users' privacy concerns, and the extent of their privacy protection behaviors, thus expanding the privacy calculus decision-making frameworks.

Israel presents a unique case for this study due to its high internet penetration rate and widespread use of social media platforms, including WhatsApp (Kemp, 2023).

The Israeli digital landscape is characterized by its diverse user base and varying levels of digital literacy, which offers a rich context for examining digital communication behaviors and privacy concerns. Understanding WhatsApp usage in this cultural and technological context will contribute to a broader global discourse on digital privacy and user behavior.

Israeli respondents provided data on their use and perceptions of WhatsApp through an online survey that included original questions on usage frequency, privacy settings, privacy importance on the platform, and demographic information. The study relies on the following hypotheses:

H1: There is a positive correlation between the frequency of WhatsApp use and the level of privacy concern among users.
H2: There is a positive correlation between the frequency of WhatsApp use and implementation of privacy protection behaviors.
H3: There is a positive correlation between the level of privacy concerns and the implementation of privacy protection behaviors among WhatsApp users.
H4: The level of privacy concerns mediates the relationship between the frequency of WhatsApp use and implementation of privacy protection behaviors among users.

Methodology

Procedure

To ensure a representative sample, participants were recruited using a stratified random sampling method, drawing from an online panel that included all demographic groups in Israel. The sample size was estimated using G*Power software (Faul et al., 2009). For a population of 6 million citizens aged 18 and over, a 95% confidence level, and a maximum margin of error of 4.5%, the required sample size was calculated to be 475 participants. However, the final sample size was 505. The questionnaire, containing 45 items, explored the use of instant messaging applications and social media, focusing specifically on WhatsApp. It assesses the usage habits of various WhatsApp features, concerns about the potential privacy harm from using WhatsApp, and measures taken to protect privacy on the platform. Most questions employed a Likert scale designed to assess the variables in the question. Moreover, the questionnaire collected sociodemographic data from the respondents.

Participants

The participant pool was 52.7% women, with 57.5% reporting being married. The participants' age ranged from 18 to 64 years, with a mean of 39.78 (*SD* = 13.03). More than half (56.5%) held a bachelor's degree, 24.5% held a high school diploma, and 19% held a master's degree or higher. More than half of the participants self-identified as secular (54.3%), whereas 45.7% identified themselves as religious. Regarding income, 22.9% were below average, 22.7% were around average income, 18.8% were above average, 17.5% were above average, and 18.1% were significantly above average.

Measurements

WhatsApp Use Frequency

WhatsApp usage frequency is the intensity and frequency of a user's engagement with an application. This independent variable was operationalized using multiple measures. The aspects of engagement considered were the frequency of logins to WhatsApp, duration of application use, number of messages sent and received daily, frequency of WhatsApp group interactions, file and photo sharing, and video and voice calls. Respondents indicated their engagement with each item on a 6-point Likert scale ranging from 1 (never) to 6 (every waking hour). The scale included nine items, each reflecting different aspects of WhatsApp usage. A satisfactory Cronbach's alpha of .85 was obtained. An index of WhatsApp usage frequency was calculated for each participant based on their composite score, with a mean score of 3.57 ($SD = .87$).

Usage of WhatsApp Features

Nine items on a Likert scale were used to measure the frequency of various WhatsApp uses reported by the participants. These items encompassed interpersonal messages, messages in groups, sending a voice message, making a phone call, using emojis, file sharing, photo sharing, video sharing, and conference calls (videos). The scale's Cronbach's alpha indicated high internal consistency ($\alpha = .849$). Based on these nine items, an index was created to measure WhatsApp usage frequency, with a mean of 3.55 ($SD = .87$).

Privacy Concerns

This variable is conceptualized as the degree to which individuals express concern about their privacy on WhatsApp. It can serve as an independent variable (privacy protection behavior) or a dependent variable (concerning the frequency of WhatsApp use). The operationalization of this variable included quantifying users' responses to survey items and eliciting their concerns regarding privacy on WhatsApp. Respondents were asked to indicate their level of concern on a Likert scale ranging from 1 (totally disagree) to 5 (completely agree). The scale consists of seven items addressing different aspects of privacy concerns: statements regarding the importance of maintaining privacy, concerns about data transfer to commercial companies, preferences for secure cloud storage, concerns about content ending up in foreign hands, preferences for privacy control features, preferences regarding read receipts, and the importance of end-to-end encryption. An adequate Cronbach's alpha score of .766 was obtained. The composite score for each participant was calculated as an index of privacy concerns, with a mean score of 3.37 ($SD = .86$).

Privacy Protection Behavior

This variable represents the variety of actions taken by users to protect their privacy while using WhatsApp and serves as the dependent variable in this study. Privacy protection behavior was measured using the following items: (1) Privacy setting for the "last seen" feature; (2) Privacy setting for the "profile picture"; (3) Privacy setting of who can add the user to groups; (4) Privacy setting for blocked contacts; and (5) Whether the user has disabled read permissions. Participants indicated the frequency of each privacy protection behavior on a Likert scale ranging from 1 (never) to 5 (always/constantly). An adequate Cronbach's alpha of .79 was obtained. The composite score for each participant was calculated as an index of privacy protection behavior, with a mean score of 2.05 ($SD = .43$), suggesting a moderate level of privacy protection behavior.

Results

In the comparative analysis of messaging app usage, a distinct preference for WhatsApp was observed, with its usage significantly surpassing that of the other platforms (see Figure 1). WhatsApp usage was nearly double that of Facebook, the next most popular service. Lesser-used platforms such as Telegram and Signal demonstrate a minority share in the market, which may reflect consumer preferences or awareness levels.

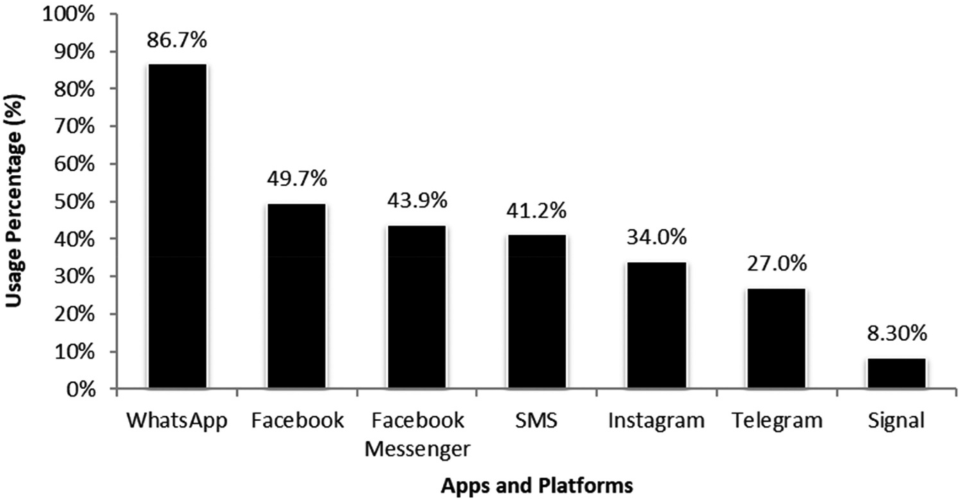

Figure 1 Usage percentage of messaging apps and social media platforms

Most respondents used WhatsApp frequently, with 45.5% using it several times daily, and 48.5% using it every hour. Interpersonal messaging was also frequent, with 41.6% of users messaging several times daily, and 33.2% messaging every hour. Group messaging was less common, with 32% of users messaging several times per day and 13% messaging every hour.

WhatsApp Feature Usage

Voice messaging was used by 21.5% of the participants several times per day and 6.4% every hour. Phone calls were less common, with 46% of participants participating infrequently and 11% participating a few times daily. Emoji use was widespread, with 41.6% utilizing them several times per day and 22% every hour. Sharing files was comparatively less frequent, with 32.5% sharing files several times per week, and 17.6% sharing files several times daily. Similarly, 29.1% shared photos several times per week and 28.1% shared photos several times per day. Video sharing was less common, with 29.7% sharing videos several times per week, and 13.5% sharing videos several times per day. The least frequent activity was conference calling, with 51% participating in using that feature rarely, and only 4.8% doing so several times daily.

In addition, a confirmatory factor analysis was conducted on nine items representing various WhatsApp modalities, using principal component analysis with varimax rotation. The adequacy of the sample size for the analysis was confirmed through the Kaiser-Meyer-Olkin measure, which yielded a value of .880, and Bartlett's test of sphericity demonstrated a significant fit to the data (χ^2 (36) = 1427.332, $p < .001$). Upon examining the PCA results, nine components were initially identified, each with eigenvalues exceeding 1. However, a closer inspection of the scree plot revealed a clear demarcation after the third component. This suggests that a three-component model was the most appropriate for the data, accounting for 68.41% of the total variance in the WhatsApp modalities (see Figure 2).

The first component extracted primarily represented WhatsApp sharing activities, encompassing "Sharing Files," "Sharing Videos," and "Sharing Photos." This factor captures the essence of WhatsApp media exchanges. The second component identified was closely tied to WhatsApp direct messaging features, including "Interpersonal Messages," "Emojis," and "Group Messaging." These elements collectively characterize a dimension of direct, often text-based communication. The third and final component distinguished itself by encapsulating live WhatsApp synchronous interactions, as evidenced by strong loadings for "Phone Calls," "Video Conferencing," and "Sending Voice Messages." This highlights the real-time interactive communication capabilities of the application.

Following these three factor loadings, we conducted a Friedman test, which indicated a significant difference in the rankings of WhatsApp usage activities: χ^2 (2) = 500.155, $p < .001$. This suggests that respondents' preferences for WhatsApp direct messaging, WhatsApp sharing activities, and WhatsApp synchronous interactions were statistically distinct.

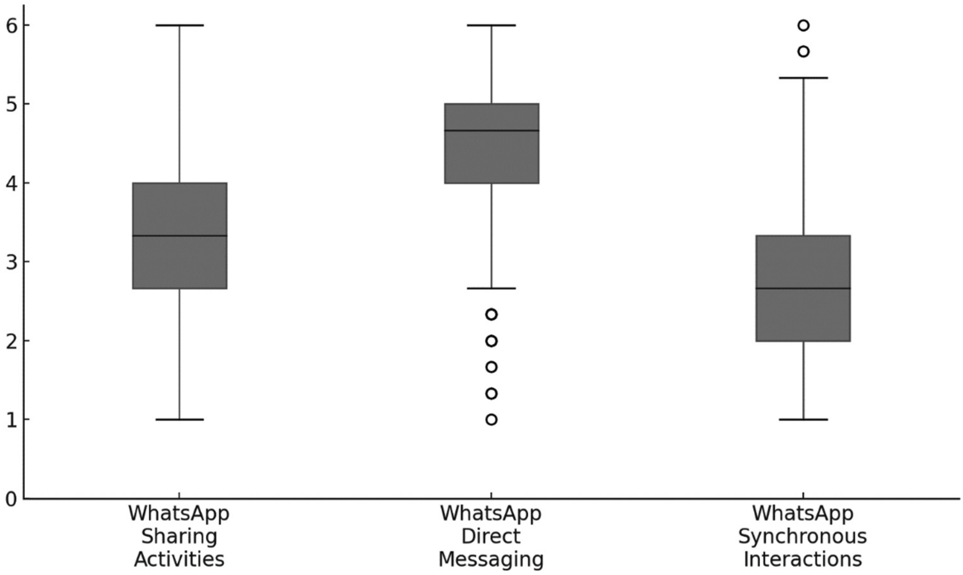

Figure 2 Component loadings for WhatsApp activity factors

Privacy Concerns

Many users valued their privacy on WhatsApp, with 73.2% agreeing largely or entirely with the sentiment. Similarly, many users (47.8%) agreed, largely or entirely, with concerns about WhatsApp transferring information to commercial companies. However, users were more divided on saving information to the cloud, with only 33.6% largely or completely agreeing, and 34.1% slightly or entirely disagreeing. Users had mixed sentiments about their chats being accessed by foreign entities, with 37.8% largely or ultimately concerned and 37.7% slightly or entirely unconcerned. Most users (51.3%) preferred privacy control settings and the majority considered end-to-end encryption to be important (65.2%).

The present study examined the relationships between the research variables using Pearson's correlation coefficients. The first hypothesis (H1) predicted a positive relationship between WhatsApp usage frequency and user privacy concerns. Correlation analysis revealed a statistically significant positive correlation between WhatsApp usage and privacy concerns ($r = .117$, $p < .05$). Thus, H1 was supported.

In addition, the factor loadings associated with WhatsApp usage displayed varying degrees of correlation with privacy concerns. Specifically, a significant positive correlation was observed between privacy concerns and WhatsApp sharing activities ($r = .103$, $p < .05$) as well as a stronger correlation with WhatsApp synchronous interactions ($r = .129$, $p < .05$). However, the correlation with WhatsApp direct messaging was not statistically significant ($r = .062$, $p > .05$).

Privacy Behaviors

The privacy settings for "last seen" were configured to "everyone" by 40.5% of users, while 34.1% set it to "nobody." For profile pictures, 61.8% set access to "everyone" and 8.5% to "nobody." Regarding group settings, the majority (70.7%) allowed "everyone" to add them to groups. Regarding contact blocking, 42.1% did not block any contacts, 40.5% blocked up to five contacts, and 17.4% blocked more than five contacts. Approximately 39.9% of the users had customized WhatsApp backgrounds, while 60.1% did not. Most users (78.5%) utilized WhatsApp's "mute forever" feature, whereas only 21.5% did not. Finally, 51.9% of users deactivated the automatic saving of photos and videos to their camera roll, whereas 48.1% did not.

The second hypothesis (H2) proposed a positive relationship between the frequency of WhatsApp use and privacy protection behaviors. However, the correlation analysis did not reveal a statistically significant relationship between these variables ($r = .037$, $p > .05$). Therefore, H2 was rejected.

H3 posited a positive relationship between privacy concerns and privacy protection behaviors among WhatsApp users. Correlation analysis indicated a statistically significant positive correlation between privacy concerns and protection behavior ($r = .525$, $p < .001$). Hence, H3 received strong support. Once again, we examined the correlation matrix between the index of privacy protection behavior and the three WhatsApp activities: sharing activities ($r = .045$, $p > .05$), direct messaging ($r = .030$, $p > .05$), and synchronous interactions ($r = .016$, $p > .05$). This indicates weak and non-significant correlations. This suggests that privacy protection behavior has little to no statistical association with WhatsApp use.

Finally, Hayes's (2022) Process Model 4, with a bootstrap of 5000 iterations, was used to examine the fourth hypothesis. H4 predicted the mediating role of the privacy concerns index in the relationship between the WhatsApp usage index (independent variable) and privacy protection behavior index (dependent variable). As illustrated in Figure 3, the results revealed a significant indirect effect of WhatsApp usage on privacy protection behaviors through privacy concerns ($\beta = .03$, $SE = .01$, 95% BootCI [0.00, 0.06]), indicating that individuals' privacy concerns mediated the relationship between WhatsApp usage and privacy protection behaviors. However, the direct effect of WhatsApp usage on privacy protection behaviors was not significant ($\beta = -.01$, $SE = .02$, $p = .54$). These findings support the mediating role of privacy concerns in the association between WhatsApp usage and individuals' implementation of privacy protection behaviors. Thus, an individual's level of privacy concerns is an essential factor influencing the relationship between their use of WhatsApp and behaviors to protect their privacy.

Furthermore, since the results were not statistically significant when assessing the direct relationship between WhatsApp use and privacy protection behaviors, we examined a combined model wherein both WhatsApp use and privacy concerns were used to predict privacy protection behaviors. Privacy concerns emerged as a significant predictor ($\beta = .267$, $p < 0.001$). Interestingly, the effect of WhatsApp use

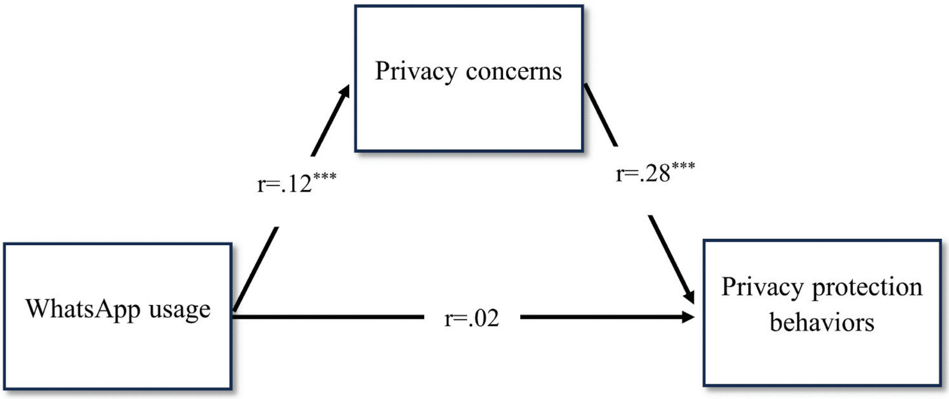

Figure 3 Mediation model
***p < .001, N = 505

on privacy protection behaviors became non-significant when privacy concerns were considered (β = −.013, $p > .05$). These findings support the mediating role of privacy concerns in the relationship between WhatsApp use and the implementation of privacy protection behaviors, underscoring the premise that while the direct effect of WhatsApp use on privacy protection behaviors is muted, its indirect effect via heightened privacy concerns is pronounced.

Discussion

Overall, the results of this study indicate the broad use of WhatsApp for multiple purposes coupled with users' varied perceptions of privacy within the platform. Son and Kim (2008) noted that recognizing threats does not intrinsically precipitate the corresponding actions. This underscores that the complexities of motivation, priority, and awareness modulate how usage patterns translate into behaviors. In the present study, although most users expressed a strong need to maintain privacy on WhatsApp, many did not adjust their privacy settings to safeguard their personal information and communication. Furthermore, the findings suggest that users may prioritize their need for connections and group participation over privacy apprehensions.

Dienlin et al. (2023) explored the privacy paradox longitudinally and uncovered an intricate relationship between privacy concerns and online behavior. The researchers differentiated between individual (within-person) and general (between-person) effects, leading to two key findings. First, individuals with heightened privacy concerns disclosed less personal information, indicating a between-person effect. More importantly, a within-person effect was observed, where sharing decreased when privacy concerns increased. These findings are relevant to our study because they highlight how specific cognitive appraisals shape online privacy actions and can explain them better than relying on general assumptions about paradoxical behaviors.

Wirth et al. (2022) provided further evidence for the privacy paradox, whereby privacy concerns failed to limit self-disclosure behaviors. Their study examined how laziness affected the relationship between privacy concerns and disclosure. Factors such as laziness help explain gaps in privacy research related to attitude-behavior inconsistencies and add to theoretical models such as the calculus framework to explain the privacy paradox. This enabled them to explain the privacy paradox in a way that went beyond existing theories, such as the privacy calculus model, which proposes that when risks outweigh benefits, people take measures to minimize exposure (Dinev & Hart, 2006).

The present study noted a positive correlation between WhatsApp usage frequency and privacy concerns. However, the link between WhatsApp usage frequency and adoption of privacy protection behaviors was insignificant. This suggests that, while increased app usage is associated with elevated privacy concerns, these apprehensions do not necessarily spur proactive privacy-protection behaviors. However, a high degree of privacy concerns correlated with an increased likelihood of protective behaviors, indicating that privacy concerns could motivate individuals to guard their privacy more diligently.

Moreover, our findings suggest that users' privacy concerns mediate WhatsApp usage and privacy protection behaviors. Hence, users' concerns with privacy significantly affect the relationship between WhatsApp usage and the enactment of protective behaviors. This finding implies that enhancing awareness of privacy issues can motivate users to actively engage in behaviors that preserve privacy, thereby reducing potential privacy risks.

Importantly, privacy concerns strongly predicted privacy protection, suggesting that threat perceptions can serve as an impetus for protective actions. This follows the logic of the privacy calculus models. Users were spurred to act as unease grew regarding WhatsApp policies and practices. However, the attitude-behavior gap in the privacy paradox shows that this is not always true. Here, concerns have a decisive impact, overriding on other motivations.

Privacy concerns are vital for WhatsApp usage and protective behaviors. Although the frequent use of WhatsApp inevitably raises privacy concerns, these apprehensions can act as crucial stimuli for enacting privacy protection behaviors, thus fostering a safer online communication environment. Considering the growing apprehensions about data privacy and the omnipresence of applications such as WhatsApp, the outcomes of this study underscore the significance of understanding user behavior and perceptions of privacy.

Limitations and Future Directions

Future studies could address these privacy concerns, as well as measures to encourage privacy-preserving behaviors among WhatsApp users. It would also be beneficial to examine potential cross-cultural differences to further refine our understanding of privacy concerns and behaviors in diverse sociocultural contexts.

Cultural values, such as individualism versus collectivism and uncertainty avoidance, significantly influence privacy perceptions and behaviors, often shaping how individuals assess risks and decide on their online activities (Engström et al., 2023). In collectivistic societies, the prioritization of group harmony and familial relationships over individual privacy may diminish the emphasis on privacy-preserving behaviors due to strong social norms favoring transparency and interconnectedness. Conversely, individualistic cultures, which emphasize personal autonomy and control, may heighten privacy concerns, potentially resulting in increased privacy-preserving behaviors.

Israel's cultural landscape, characterized by a strong familial culture, high stress levels, and substantial immigration, reflects a close relationship between parents and adolescents. Israeli parents often adopt proximal parenting styles suitable for collectivistic cultural settings, particularly in hazardous environments (Scharf, 2014). Despite some convergence among various socio-ethnic groups, significant disparities persist in all aspects of family life, maintaining an extensive diversity in family arrangements and lifestyles. The organizational structure of families in Israel is influenced by modernization and Westernization, yet enduring traditional principles continue to have a considerable impact (Lavee & Katz, 2003). Thus, examining such and other sociocultural settings using multimethod designs can also be insightful. Additionally, incorporating other variables alongside privacy concerns could further unpack drivers of protection behavior.

Furthermore, our research focused on statistical correlations and patterns within a representative sample. Although robust in identifying general trends and relationships, this approach does not capture the nuanced motivations and contextual factors provided by a qualitative approach. Future research could benefit significantly from incorporating qualitative methods, such as in-depth interviews or focus groups, to investigate the reasons behind users' privacy concerns and protection behaviors. Qualitative data could enrich our understanding of the motivations for proactive or avoidant behaviors regarding privacy-safeguarding activities on WhatsApp and in a broader online environment. Recent studies, such as those by Sur and Goswami (2021) and Singh and Mishra (2020), highlight the complex interplay between digital privacy concerns and user behavior, suggesting that qualitative insights can provide a more comprehensive understanding of these dynamics. By integrating qualitative and quantitative approaches, future research could offer a more holistic view of privacy, informing more effective policymaking and user education strategies.

Our findings provide a useful foundation for ongoing inquiries on technology use, privacy perceptions, and related outcomes. However, it has several important implications. Users highlight the need for ongoing vigilance as WhatsApp becomes further enmeshed in communication. For platforms, the results underscore the value of bolstering trust and transparency in data practices to mitigate privacy concerns. More broadly, the analysis enriches the theoretical understanding of how usage, perceptions, and behaviors interrelate while demonstrating the key role of perceived threats.

The insights from this study can help shape policies and procedures that improve user privacy protection on WhatsApp and other platforms by uncovering the factors influencing users' attitudes and behaviors toward privacy. In addition, it provides a novel perspective on the utilization of WhatsApp in Israel, a subject that has not been examined in previous research. The outcomes of this study have implications for future research on privacy issues surrounding instant messaging applications and their impact on user behavior. These insights highlight the need for more robust policies and procedures to protect user privacy on WhatsApp and similar messaging applications, particularly interpersonal communication. Policymakers should consider regulations extending beyond encryption, including metadata protection, transparent data usage, and minimized data retention. Developing intuitive, user-centric privacy controls and promoting educational campaigns are essential for bridging the gap between privacy concerns and protective behaviors. Furthermore, fostering platform interoperability can reduce user dependency and encourage privacy-centric competition. These measures can significantly enhance user privacy protection and ensure a safer digital communication environment.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

ORCID

Yaron Ariel http://orcid.org/0000-0002-9705-5416
Eilat Chen Levy http://orcid.org/0000-0002-9119-2591

References

Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *2nd Annual Workshop on Economics and Information Security-WEIS*, University of Maryland, College Park, USA (Vol. 3, pp. 1–27).

Ahad, A. D., & Lim, S. M. A. (2014). Convenience or nuisance? The 'WhatsApp' dilemma. *Procedia-Social and Behavioral Sciences*, 155, 189–196. https://doi.org/10.1016/j.sbspro.2014.10.278

Aizenkot, D., & Kashy-Rosenbaum, G. (2018). Cyberbullying in WhatsApp classmates' groups: Evaluation of an intervention program implemented in Israeli elementary and middle schools. *New Media & Society*, 20(12), 4709–4727. https://doi.org/10.1177/1461444818782702

Avidar, R., Ariel, Y., & Elishar-Malka, V. (2017). Wartime changes in news consumption patterns among Israeli WhatsApp users: Operation protective edge as a case study. In D. Rubinstein

& D. Caspi (Eds.), *Reporting the Middle East: Challenges and chances* (pp. 79–98). World Scientific Publishing.

Awwad, A. (2021). The impact of over the top service providers on the global mobile telecom industry: A quantified analysis and recommendations for recovery. ArXiv Preprint ArXiv:2105.10265. https://doi.org/10.48550/arXiv.2105.10265

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

Brandtzaeg, P. B., & Lüders, M. (2018). Time collapse in social media: Extending the context collapse. *Social Media + Society*, 4(1), 1–10. https://doi.org/10.1177/2056305118763349

Ceci, L. (2023). *Monthly global unique WhatsApp users 2020-2023*. https://www.statista.com/statistics/1306022/whatsapp-global-unique-users

Chen, M., & Peng, A. Y. (2023). Why do people choose different social media platforms? Linking use motives with social media affordances and personalities. *Social Science Computer Review*, 41(2), 330–352. https://doi.org/10.1177/08944393211049120

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Dahabiyeh, L., Farooq, A., Ahmad, F., & Javed, Y. (2023). Explaining technology migration against the change in terms of use: An fsQCA approach. *Information Technology & People*, 37(3), 1073–1102. https://doi.org/10.1108/ITP-07-2022-0498

Daradkeh, M. (2023). The link between privacy and disclosure behavior in social networks. In M. Husain, M. Faisal, H. Sadia, T. Ahmad, & S. Shukla (Eds.), *Advances in Cyberology and the advent of the next-gen information revolution* (pp. 38–61). IGI Global. https://doi.org/10.4018/978-1-6684-8133-2.ch003

Dienlin, T., Masur, P. K., & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *New Media & Society*, 25(5), 1043–1064. https://doi.org/10.1177/14614448211016316

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. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Engström, E., Eriksson, K., Björnstjerna, M., & Strimling, P. (2023). Global variations in online privacy concerns across 57 countries. *Computers in Human Behavior Reports*, 9, 1–9. https://doi.org/10.1016/j.chbr.2023.100268

Farooq, A., Dahabiyeh, L., & Javed, Y. (2024). When WhatsApp changed its privacy policy: Explaining WhatsApp discontinuation using an enablers-inhibitors' perspective. *Online Information Review*, 48(1), 22–42. https://doi.org/10.1108/OIR-04-2022-0232

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G* power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, 41(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Fiesler, C., & Hallinan, B. (2018). We are the product: Public reactions to online data sharing and privacy controversies in the media. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–13. https://doi.org/10.1145/3173574.3173627

Griggio, C. F., Nouwens, M., & Klokmose, C. N. (2021). Caught in the network: The impact of WhatsApp's 2021 privacy policy update on users' messaging app ecosystems. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 104, 1–23. https://doi.org/10.1145/3491102.3502032

Griggio, C. F., Nouwens, M., & Klokmose, C. N. (2022). Caught in the network: the impact of WhatsApp's 2021 privacy policy update on users' messaging app ecosystems. *Proceedings of the 2022 CHI conference on human factors in computing systems (CHI'22)*, New York (pp. 1–23). ACM Press.

Guo, J., Li, N., Wu, Y., & Cui, T. (2020). Examining help requests on social networking sites: Integrating privacy perception and privacy calculus perspectives. *Electronic Commerce Research and Applications*, 39(1), 100–112. https://doi.org/10.1016/j.elerap.2019.100828

Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach* (3rd ed.). The Guilford Press.

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. https://doi.org/10.1089/cyber.2012.0041

Johns, A., & Cheong, N. (2021). The affective pressures of WhatsApp: From safe spaces to conspiratorial publics. *Continuum: Lifelong Learning in Neurology*, 35(5), 732–746. https://doi.org/10.1080/10304312.2021.1983256

Kemp, S. (2023). *Digital 2023: Israel*. https://datareportal.com/reports/digital-2023-israel

Kordzadeh, N., Warren, J., & Seifi, A. (2016). Antecedents of privacy calculus components in virtual health communities. *International Journal of Information Management*, 36(5), 724–734. https://doi.org/10.1016/j.ijinfomgt.2016.04.015

Kustijono, R., & Zuhri, F. (2018). The use of facebook and WhatsApp application in learning process of physics to train students' critical thinking skills. *IOP Conference Series: Materials Science & Engineering*, 296(1). https://doi.org/10.1088/1757-899X/296/1/012025

Lavee, Y., & Katz, R. (2003). The family in Israel. *Marriage & Family Review*, 35(1), 193–217. https://doi.org/10.1300/J002v35n01_11

Liu, L., Roche, D. S., Theriault, A., & Yerukhimovich, A. (2022). Fighting fake news in encrypted messaging with the fuzzy anonymous complaint tally system (FACTS). In *Proceedings 2022 Network and Distributed System Security Symposium* (pp. 1–17). San Diego, CA, USA. https://doi.org/10.48550/arXiv.2109.04559

Mars, M., Morris, C., & Scott, R. E. (2019). WhatsApp guidelines – what guidelines? A literature review. *Journal of Telemedicine and Telecare*, 25(9), 524–529. https://doi.org/10.1177/1357633X19873233

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Massara, F., Raggiotto, F., & Voss, W. G. (2021). Unpacking the privacy paradox of consumers: A psychological perspective. *Psychology & Marketing*, 38(10), 1814–1827. https://doi.org/10.1002/mar.21524

Masur, P. K. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

Mols, A., & Pridmore, J. (2021). Always available via WhatsApp: Mapping everyday boundary work practices and privacy negotiations. *Mobile Media & Communication*, 9(3), 422–440. https://doi.org/10.1177/2050157920970582

Olaniyi, O., & Omubo, D. S. (2023). WhatsApp data policy, data security and users' vulnerability. *International Journal of Innovative Research & Development*, 12(2). https://ssrn.com/abstract=4546203

Rastogi, N., & Hendler, J. (2017). WhatsApp security and role of metadata in preserving privacy. *International Conference on Cyber Warfare and Security arXiv*, 1701(6817), 269–275. https://doi.org/10.48550/arXiv.1701.06817

Santos, M., & Faure, A. (2018). Affordance is power: Contradictions between communicational and technical dimensions of WhatsApp's end-to-end encryption. *Social Media+ Society*, 4(3), 1–16. https://doi.org/10.1177/2056305118795876

Scharf, M. (2014). Parenting in Israel: Together hand in hand, you are mine, and I am yours. 193-206. In H. Selin (Ed.), *Parenting across cultures* (pp. 193–206). Springer. https://doi.org/10.1007/978-94-007-7503-9_14

Schnitzler, T., Kohls, K., Bitsikas, E., & Pöpper, C. (2022). Hope of delivery: Extracting user locations from mobile instant messengers. *arXiv*. https://doi.org/10.48550/arXiv.2210.10523

Singh, K., & Mishra, S. (2020). Mapping the inter-relation of abuse of dominant position and merger control regime vis-à-vis big data: The curious case of WhatsApp privacy policy. *Journal of National Law University Delhi*, 7(1–2), 53–75. https://doi.org/10.1177/22774017221098800

Son, J. Y., & Kim, S. S. (2008). Internet users' information privacyprotective responses: A taxonomy and a nomological model. *MIS Quarterly*, *32*(3), 503–529. https://doi.org/10.2307/25148854

Stevic, A., Schmuck, D., Koemets, A., Hirsch, M., Karsay, K., Thomas, M., & Matthes, J. (2022). Privacy concerns can stress you out: Investigating the reciprocal relationship between mobile social media privacy concerns and perceived stress. *Communications*, 47(3), 327–349. https://doi.org/10.1515/commun-2020-0037

Sundaram, R., & Shetty, S. (2022). Privacy concerns and protection behavior during the covid-19 pandemic. *Problems and Perspectives in Management*, 20(2), 57–70. https://doi.org/10.21511/ppm.20(2).2022.06

Sur, S., & Goswami, K. (2021). Digital privacy: Case study analysis on whatsapp privacy policy changes. *International Journal of Applied Science and Engineering*, 9(2), 157–167. https://doi.org/10.30954/2322-0465.2.2021.4

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

Talwar, A., Chaudhary, A., & Kumar, A. (2022). Encryption policies of social media apps and its effect on user's privacy. *10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 1–4. https://doi.org/10.1109/ICRITO56286.2022.9964730

Tan, E. Y. Q., Wee, R. R. E., Wee Ern, S. Y., Heng, K. J. Q., Chin, J. W. E., Tong, E. M. W., & Liu, J. C. J. (2021). Tracking private WhatsApp discourse about COVID-19 in Singapore: Longitudinal infodemiology study. *Journal of Medical Internet Research*, 23(12), e34218. https://doi.org/10.2196/34218

Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. *Journal of Enterprise Information Management*, 34(4), 1097–1120. https://doi.org/10.1108/JEIM-03-2020-0088

Treré, E. (2018). The sublime of digital activism: Hybrid media ecologies and the new grammar of protest. *Journalism & Communication Monographs*, 20(2), 137–148. https://doi.org/10.1177/1522637918770435

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. https://doi.org/10.1177/0270467607311484

Tunjera, N. (2023). Adopting WhatsApp to reduce transactional distance during the COVID-19 pandemic. *Electronic Journal of E-Learning*, 21(2), 110–120. https://doi.org/10.34190/ejel.21.2.2752

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 6(1), Article 3. https://doi.org/10.5817/CP2012-1-3

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Wiener, A., & Stegman, O. (2023). *Social media and digital platforms use in Israel*. https://en.isoc.org.il/data-and-statistics/social_media_use_il_2023

Wijnberg, D., & Le-Khac, N. A. (2021). Identifying interception possibilities for WhatsApp communication. *Forensic Science International: Digital Investigation*, 38, 301132. https://doi.org/10.1016/j.fsidi.2021.301132

Wirth, J., Maier, C., Laumer, S., & Weitzel, T. (2022). Laziness as an explanation for the privacy paradox: A longitudinal empirical investigation. *Internet Research*, 32(1), 24–54. https://doi.org/10.1108/INTR-10-2019-0439

Yu, L., Li, H., He, W., Wang, F.-K., & Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51, 51. https://doi.org/10.1016/j.ijinfomgt.2019.09.011