Issues in Informing Science + Information Technology

An Official Publication of the Informing Science Institute
InformingScience.org

IISIT.org

Volume 22, 2025

FACTORS INFLUENCING ONLINE IDENTITY FALSIFICATION AMONG ISRAELI STUDENTS IN THE WAKE OF THE COVID-19 PANDEMIC

Maor Weinberger*	Bar-Ilan University, Ramat-Gan, Israel	maor89@gmail.com
Dan Bouhnik	Jerusalem College of Technology, Jerusalem, Israel	bouhnik@jct.ac.il

* Corresponding author

ABSTRACT

Aim/Purpose	The research examines the main factors that motivate users to provide falsified details upon website registration and identifies the types of personal details that are most prone to falsification. In addition, the tendency for identity falsification is predicted by examining various factors, such as, sense of online anonymity, privacy concern, and socio-demographic factors. To provide a contemporaneous dimension to the research, those issues are investigated in relation to the COVID-19 pandemic and examine its influence on privacy concerns and the willingness to expose personal details.
Background	Many users choose to deliberately falsify their details during online activities.
Methodology	To assess this claim, a user study was carried out among 245 students of the Israeli academia, comprising 52.2% men and 47.8% women, with ages ranging from 18 to 60 years. The research applied a quantitative method using online closed-ended questionnaires. The results were analyzed using conventional statistical methods, such as t-tests and ANOVA. To predict the tendency of identity falsification upon website registration, a logistic regression analysis was performed, taking into account various independent variables: sense of anonymity on websites; sense of exposure to other users online; privacy concern; Internet proficiency; various demographic factors: gender, age, and education.
Findings	The research findings suggest that privacy-related issues are the most prevalent for identity falsification. In addition, logistic regression showed that the higher the privacy concerns rates, the higher the chance for identity falsification.

Editor: Eli Cohen | Received: September 25, 2024 | Revised: April 10, April 15, 2025 | Accepted: April 28, 2025
Cite as: Weinberger, M., & Bouhnik, D. (2025). Factors influencing online identity falsification among Israeli students in the wake of the COVID-19 pandemic. *Issues in Informing Science and Information Technology, 22,* Article 8. https://doi.org/10.28945/5513

Recommendations for Practitioners	Website operators and online marketers should adapt the research findings and increase their transparency regarding the use of the information being collected, to increase the trust among users and eliminate privacy concerns. This will help them maintain good customer relations, which may benefit them and the consumers in the long run. In addition, local governments and internet regulators should formulate adequate laws and binding guidelines to force website operators and online marketers to take the necessary steps for reducing privacy concerns among internet consumers.
Impact on Society	The research may bear social implications for website operators and online marketers who, by recognizing the reasons behind identity falsification, may create more balanced personalization mechanisms for their own benefit and the benefit of their consumers.
Future Research	Due to the limitation of the findings, further investigation should apply the proposed methodology to additional population types, in various age groups, cultures, and countries of origin.
Keywords	identity falsification, privacy concern, self-disclosure, online anonymity, trust, COVID-19

INTRODUCTION

The extensive growth of information-gathering mechanisms and the improved capabilities to store and process vast amounts of personal information for online marketing purposes have turned online users' data into an asset and even a tradable commodity (Chegarova & Wang, 2019; Dinev & Hart, 2005). Both commercial and service websites today request information from their visitors and/or customers (Bandara et al., 2020; Zeng et al., 2021). Although search and transaction data can be easily collected by website operators, users' personal information needs to be provided by the users themselves and is considered a key to building a competitive advantage.

Information gathered regarding users' habits and preferences is being used by marketers and other online entities to personalize their services and adapt them to the specific user needs, to maximize their profits (Chellappa & Sin, 2005; Cloarec, 2020; Malheiros et al., 2013; Poddar et al., 2009; Zeng et al., 2021). The personalization of online services may also be beneficial for the users, as it increases their sense of control through order tracking and email notifications and also allows them to receive recommendations for products that are based on their liking (Karwatzki et al., 2017). However, users' agreement for self-disclosure necessarily entails a certain relinquishment of their privacy, and some may forfeit the benefits of personalization if they are more concerned about the potential misuse of their personal information (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Sutanto et al., 2013; Zeng et al., 2021). This is a commonly discussed tradeoff in the literature termed the personalization-privacy tradeoff (Karwatzki et al., 2017; Weinberger et al., 2017), and it reflects the equilibrium between self-disclosure and privacy protection. As Bandara et al. (2020) state: "there is a fine line between data-driven marketing efforts… and protection of consumer privacy" (p. 1). When this line is crossed, users may choose not to disclose their personal information, withhold the information, or provide false information (Miltgen & Smith, 2019).

Research indicates that many individuals intentionally provide false information during online interactions and register on websites using entirely fabricated details to gain unauthorized access to online services (Punj, 2017; Rainie et al., 2013). However, this behavior can also be interpreted as a form of privacy protection employed by users to safeguard their personal information. Previous studies exploring this phenomenon have identified privacy-related concerns as primary reasons for individuals withholding personal details or submitting falsified information upon website registration. These concerns include distrust towards website operators and concerns about potential misuse of personal

data (Acquisti et al., 2015; Miltgen & Smith, 2019), as well as perceptions of unethical practices by companies (Punj, 2017). These factors consistently rank high among the motivations for identity falsification (Weinberger & Bouhnik, 2019).

The emergence of the COVID-19 pandemic in December 2019 has heightened apprehensions about the unauthorized use of personal information. Governments have intensified surveillance measures aimed at prioritizing public health over privacy concerns (Smidt & Jokonya, 2021). This has made individuals more reluctant to share their personal data (Fu et al., 2020) and has led to an increase in privacy-protective behaviors, including identity falsification.

This research seeks to explore the primary motivations and factors that lead users to provide inaccurate information when requested by websites. Additionally, the research aims to identify which specific types of personal information are most likely to be falsified. It examines both privacy-related factors that were proven as antecedents for identity falsification and underexplored factors, including social-psychological determinants, such as a desire to take revenge on the website operators.

Thus, the main research question that this research seeks to answer is: What are the main factors for online identity falsification? (**RQ1a**) And what types of personal details are most prone to falsification? (**RQ1b**). As socio-demographic factors were also found in the past to be associated with privacy-protective behavior (e.g., Dinev & Hart, 2005; Thelwall & Vis, 2017), this research examined: whether and to what extent do socio-demographic factors (gender, age, and education) and Internet proficiency predict the tendency for identity falsification? (**RQ2**). In addition, as privacy concerns were found to positively affect privacy-protective behavior (Sutanto et al., 2013), such as identity falsification, the research seeks to answer: whether and to what extent do privacy-related issues, such as privacy concern and sense of online anonymity, predict the tendency for identity falsification? (**RQ3**).

Furthermore, as will be elaborated next, past literature found that COVID-19-related government surveillance influences privacy-protective behavior and the willingness to comply with government mitigation efforts (Chan & Saqib, 2021). Therefore, the study also examined whether the COVID-19 pandemic affected people's privacy concerns and their willingness to share personal information, and if so, to what extent (**RQ4**).

Previous research has shown that when more sensitive information is collected, it tends to increase privacy concerns. This increased concern often leads individuals to place less emphasis on social benefits or the common good (Kim & Kwan, 2021) and makes them more reluctant to disclose their personal details (Fu et al., 2020). Thus, this research attempts to link the tendency not to comply with epidemiological investigations during the COVID-19 pandemic and the tendency towards online identity falsification. It investigates: what are the main factors not to comply with epidemiological investigations, and are they different from those of online identity falsification? (**RQ5**).

The cost of refraining from personalization and adopting privacy-protective behavior, such as identity falsification, might be high for both marketers and consumers. On the one hand, it prevents companies from creating accurate profiles of their customers to potentially maximize their profit (Poddar et al., 2009), and on the other hand, consumers may lose potential benefits (Cloarec, 2020). Therefore, by recognizing the reasons behind identity falsification, the research may help to create more balanced personalization mechanisms, which will benefit both sides – marketers and consumers as one.

RELATED WORK

The literature review will consist of four scopes: first, it explores the issue of information disclosure as a tool for online marketers; second, it reviews the existing literature that examined online privacy concerns and the resultant privacy-protective behavior; third, the literature review surveys the determinants for identity falsification as found in previous studies; finally, the influence of the COVID-19 pandemic on the issues of privacy concern and self-disclosure is discussed.

Information Disclosure as a Tool for Online Marketers

Online commercial interactions between consumers and marketers are prominently based on the disclosure of personal information (Bandara et al., 2020; Dinev & Hart, 2005; Zeng et al., 2021). Companies constantly analyze the online activities of their customers to understand their buying habits and preferences (Punj, 2017). The information gathered is used to personalize advertisements and product suggestions that are adapted to the customers' needs (Bandara et al., 2020; Poddar et al., 2009; Zeng et al., 2021). This may make a significant contribution to the increase in customer satisfaction and loyalty (Chellappa & Sin, 2005). Personalization may also be beneficial for consumers, as it increases their sense of control through order tracking and also allows them to receive recommendations for products that are based on their personal preferences (Karwatzki et al., 2017). In addition, they can predefine an instant alert to be sent to them in case of a price drop in their desired product (Chellappa & Sin, 2005).

This exchange of information between the consumers and marketers is governed by principles of informed consent from the consumers' side and fair information use from the companies' side. The Federal Trade Commission (FTC) has set up five core principles to provide instructions to online businesses on how to act to increase online commerce: notice; choice; access; security; and redress. This includes their guarantee to keep the collected information secure, and the application of enforcement mechanisms through regulations or other means, to ensure compliance. When consumers feel that their personal information is not being used according to these principles, it may elevate their privacy concerns (Sheehan & Hoy, 2000). Privacy protection regulations, such as the European Union's General Data Privacy Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Lei Geral de Proteção de Dados in Brazil, were discovered to increase consumer perception of data protection in countries in which they were implemented (Perdereaux-Weekes, 2021) due to the elevated sense of control over the data. However, these privacy policies are vague and ambiguous (Chen et al., 2021), and thus, this perceived sense of control was found to be limited among online consumers. As a result, they often favor their convenience over complying with privacy protection regulations (Zhang et al., 2024).

The equilibrium between self-disclosure and privacy protection is widely discussed in the literature in the context of the personalization-privacy tradeoff (Karwatzki et al., 2017; Weinberger et al., 2017). Consumers always weigh the risks and benefits of disclosing their personal information to online marketers in exchange for receiving a personalized service. They may favor the benefits of online personalization, as long as it does not exceedingly violate their privacy, but also might forfeit those benefits if they are more concerned about the potential misuse of the personal information (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Sutanto et al., 2013; Zeng et al., 2021).

The emergence of technologies based on artificial intelligence and Internet of Things devices (IoT), such as drones, robots, autonomous cars, and generative-AI platforms, have also added to this dilemma, since, while these technologies may bear many benefits for the life convenience of individuals, they also raise new concerns regarding user privacy (Conger et al., 2013). These technological devices harvest information about their users, which can be detected and monitored by remote servers (Yun et al., 2019). In addition, big data mining tools enable data collection agencies to efficiently analyze vast amounts of data and extract deeper insights about users, which might further endanger their privacy (Altman et al., 2018).

Privacy Concern as a Trigger of Privacy-Protective Behavior

The factors influencing users' privacy concerns were explored in numerous studies (e.g., Bansal et al., 2016; Dinev & Hart, 2005; Wills & Zeljkovic, 2011). Socio-demographic factors, such as age and education level, were found to be significant by Sheehan (2002). In terms of gender, Thelwall and Vis (2017) found that women are more concerned with their online privacy than men and tend to engage more in privacy-protective behavior. Dinev and Hart (2005) found that users with higher levels of Internet literacy have lower levels of privacy concern. Users' characteristics, such as agreeableness,

conscientiousness, and openness (Junglas et al., 2008), and their level of trust (Bansal et al., 2016; Wirtz & Lwin, 2009) were also found to be correlated with privacy concern.

Previous studies also showed that privacy concerns negatively affect users' intention to disclose their personal information online (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Sheng et al., 2008; H. J. Smith et al., 2011) and increase the likelihood of privacy-protective behavior (Sutanto et al., 2013). According to Poddar et al. (2009), when personal information is requested in online exchanges, users tend to follow three *rules of engagement*: 1) the criticality of exchange – the level of perceived necessity of the information requested; 2) felt invasion – the level of invasiveness being felt by the users; 3) fair play – the perceived fairness of the request. When users feel that one or more of these rules are broken, they may initiate a privacy-protective behavior. According to the taxonomy suggested by Son and Kim (2008), people tend to engage in privacy-protective behavior in six different ways that can be divided into three groups: 1) Information provision – refusing to share information or misrepresenting the information; 2) Private action – actively removing their data from the website or sharing a negative review to acquaintances; 3) Public action – complaining directly to the company or complaining indirectly to third-party organizations. In a later study, Nissenbaum (2011) introduced a contextual approach to privacy preservation, asserting that users feel their privacy is violated when the information requester does not keep the norms governing different social contexts, which might result in protest and complaints. H. J. Smith et al. (2011) developed a comprehensive macro model (APCO - Antecedents-Privacy Concerns-Outcomes) that takes into account various factors influencing privacy concerns (e.g., prior experience, privacy awareness, demographic and cultural factors, and personality traits), which in turn affect the intention to disclose personal information.

The Graphic, Visualization, and Usability Center's (GVU) 7th WWW User Survey revealed that approximately 40% of the respondents provided false information upon website registration, while about 15% were found to provide falsified information over 25% of the time (Kehoe & Pitkow, 1997). The numbers even seem to increase in later surveys and studies (Miltgen & Smith, 2019; Rainie et al., 2013). Rainie et al. (2013) found that 86% of American Internet users have acted to remove or mask their digital activity – 26% used a temporary username or email address, and 18% used a fake or untraceable username. Another survey found that the most frequently falsified personal details are phone number (27%); date of birth (17%); email (16%); address (15%); and name and age (14%) (Ismail, 2018, as cited in Chegarova & Wang, 2019).

Determinants for Identity Falsification

Numerous studies have explored the issue of identity falsification, highlighting privacy concerns and the desire for control over personal data as primary factors (Fox et al., 2000; Poddar et al., 2009; Rainie et al., 2013). According to Rainie et al. (2013), individuals often mask their identities online to safeguard their privacy, a method characterized by Fox et al. (2000) as a "guerilla tactic" in defense of privacy. A significant reason people resist online registration is uncertainty about how their data will be used, a concern noted since early research (Kehoe & Pitkow, 1997) and reiterated in subsequent studies that emphasize trust issues with websites and their operators (Acquisti et al., 2015; Miltgen & Smith, 2019). Another issue is the loss of control over private data, as online exchanges are remote by nature, and thus, the consumers have limited physical control over them (Poddar et al., 2009), which they try to regain. This complies with the Equity Theory that suggests consumers are using strategies that help them overcome the loss of control and restore the balance in the relationship between them and the companies (Adams, 1963). Another trigger found for privacy-protective behavior is past experience with privacy violations (Poddar et al., 2009), as users who have suffered before from privacy invasion are more likely to be cautious when asked to disclose their personal information. This corresponds with other studies that investigated the effect of online privacy literacy (OPL), i.e., knowledge of the tools available to protect their information online and Internet experience (Park, 2013; Trepte et al., 2015; Weinberger et al., 2017), on the intent to engage in self-disclosing behavior.

Previous studies have also revealed that consumers are reluctant to disclose their true identities unless they perceive significant benefits (Rainie et al., 2013). However, they often compromise their online privacy and anonymity when they believe that the advantages of revealing personal information outweigh their concerns (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Sheng et al., 2008). This behavior aligns with the concept of balancing personalization and privacy (Karwatzki et al., 2017; Weinberger et al., 2017) and is consistent with the Uses and Gratification Theory, which suggests that consumers disclose information to gain social benefits rather than forfeiting them (Debatin et al., 2009; Trepte et al., 2015).

However, the effect of privacy concerns on privacy-protective behavior was also found to be non-significant (Son & Kim, 2008). Therefore, Sannon et al. (2018) concluded that there are other determinants for this type of behavior. Identity falsification may be considered an act of defensive reaction to perceived unethical conduct by companies and may even be driven by users' anger or willingness to protest and take revenge on the website that hassles them with personal questions before revealing the information they seek (H. Li et al., 2019; Poddar et al., 2009). This type of behavior may also be an attempt to avoid unsolicited advertising (Malheiros et al., 2013), as consumers today understand that sharing truthful information may result in unwanted communications or spam (Poddar et al., 2009). In addition, this behavior can be affected by users' general attitudes about lying and deception online (Sannon et al., 2018). Bouhnik and Deshen (2014) found the falsification of personal information as one kind of unethical behavior conducted among youth in the Internet environment, as well as harassment and plagiarism.

Finally, studies found that socio-demographic factors are also likely to influence the decisions to falsify or conceal personal information online. Punj (2017) claimed that consumers with higher education or higher income may have a stronger tendency to falsify personal information. Younger consumers (under 30) were found to be more engaged in falsifying information, compared to older consumers (Poddar et al., 2009), even though Punj (2017) conversely claims they are less inclined to do so. In addition, even though women were found to be more concerned with their online privacy than men (Wills & Zeljkovic, 2011), they were also found to publish more personal information than men (Acquisti & Gross, 2006; Fogel & Nehmad, 2009; Thelwall & Vis, 2017) and rarely adopt privacy protection behavior (Yao & Linz, 2008). Men were also found to protest more against online technology companies than women (H. Li et al., 2019). Some studies also addressed the influence of culture on users' tendency to disclose information online. Posey et al. (2010) found that users in individualistic countries disclose less personal information in social media than in collectivistic countries, and Y. Li et al. (2022) strengthen this claim by determining that American users disclose less information than those in Korea and China.

The Influence of the COVID-19 Pandemic on the Issues of Privacy Concern and Self-Disclosure

The emergence of the COVID-19 pandemic in December 2019 led to a shift in attitudes toward privacy (Ahn et al., 2020; Jung et al., 2020; Kim & Kwan, 2021; Smidt & Jokonya, 2021), prompting a reevaluation of privacy considerations. Governments have tried to stop or slow down the spread of the virus using various methods, including the increase of surveillance of their citizens in ways that prioritize lifesaving over privacy preservation (Smidt & Jokonya, 2021). For example, one of the most popular methods to enforce social distancing and detect and isolate confirmed cases is "contact tracing", which "involves identifying, listing, and taking follow-up action with the contacts" of an infected person (Jung et al., 2020). This can be done manually by conducting private interviews with confirmed patients (Ahn et al., 2020) or by using smartphone applications relying on Bluetooth technology that detects the proximity of an infected person to others (Chan & Saqib, 2021). Countries like Taiwan and Singapore authorized the remote monitoring of quarantine orders. Israel implemented "digital epidemiological investigations" to locate potential contacts of infected individuals (Amit et al., 2020).

However, as the application of surveillance technologies on the civilian population may be efficient in identifying potential contacts and benefit public safety, it uses personally identifiable information (PII) with limited restrictions, potentially jeopardizing the privacy of patients and their contacts (Ahn et al., 2020; Amit et al., 2020; Jung et al., 2020). Smidt and Jokonya (2021) found that government surveillance elevates public privacy concerns, which were found to lower public compliance with the government mitigation efforts, reflected in the reluctance to download contact tracing apps (Chan & Saqib, 2021). Xing et al. (2021) discovered that public views on national policies and efforts to mitigate crises are influenced by both concerns about privacy and cultural factors. The level of these concerns was also discovered to be different in each country. For example, while US citizens expressed concerns about government use of dedicated mobile contact-tracing apps during the pandemic (Ioannou & Tussyadiah, 2021), Israeli citizens showed apathy towards government surveillance (Duke, 2021).

Compliance from the public is crucial for effectively controlling pandemics (French, 2011). However, because the data collected is sensitive, it raises privacy concerns. This can cause individuals to prioritize their personal privacy over societal benefits and the common good (Kim & Kwan, 2021), leading to reluctance in sharing personal information (Fu et al., 2020). Consequently, this may compromise the integrity and accuracy of the data disclosed. Inaccurate information gathered from epidemiological studies could result in incorrect assessments regarding strategies to contain the outbreak (Ahn et al., 2020).

This research will build upon this assertion and will try to identify the factors for non-compliance with epidemiological investigations and their similarities or differences from those of online identity falsification.

As Miltgen and Smith (2019) claim, "Despite the obvious importance of the topic of falsification, surprisingly little attention has been paid to this topic in the IS literature" (p. 699). Therefore, this study aims to contribute to this underexplored area by examining various factors influencing the deliberate creation of fake identities in response to website requests.

Initial exploratory research was conducted as a pilot to investigate what prompts users to withhold their information or resort to creating fake identities and providing false information during website registration (Weinberger & Bouhnik, 2019). This research was approached from a perspective that considers privacy threats, aiming to understand the central role of the desire for online anonymity among other factors that lead to non-disclosure of personal details or identity falsification. The desire to maintain anonymity emerged as a predominant motive for such behavior, although it alone did not reliably predict tendencies towards non-disclosure or identity falsification during website registration.

Therefore, it seems there are other determinants for this type of behavior other than privacy concerns, or as Sannon et al. (2018) phrased it, "privacy concerns do not explain the whole story" (p. 2). Accordingly, this research strives to find other determinants for this kind of behavior, including social-psychological determinants, such as a desire to take revenge on the website operators.

This research will be based on the above pilot research and build upon the findings of relevant past literature (e.g., Miltgen & Smith, 2019; Poddar et al., 2009; Punj, 2017) to understand users' intentions to obscure and falsify their online identity. This research will also strive to detect the exact types of personal details that are most prone to falsification. This will be done by investigating the different approaches consumers use to manage their personal information online, depending on their privacy concerns and sense of anonymity, but also their Internet proficiency and socio-demographic factors. Finally, this research will examine the potential influence of the COVID-19 pandemic on the issues of privacy concern and willingness to expose personal details.

METHODS

SAMPLE POPULATION

This research involved 245 students from Israeli academic institutions, comprising 52.2% men and 47.8% women, with ages ranging from 18 to 60 years. It utilized a quantitative approach through online closed-ended questionnaires that the participants were asked to complete during their academic courses of the 2020-21 school year. The quantitative method allows the gathering of large amounts of data in a short time and analyzing them using conventional statistical tools. The distribution of online questionnaires was essential, as the research was conducted under COVID-19 restrictions. However, to minimize falsified and misrepresented responses, the participating students were first instructed during class hours (remotely) about the questionnaire and were able to approach the course instructor in case of any issues. The choice of students as the research population was made due to their relatively higher digital orientation and proficiency in the online environment. Thus, the research themes should be more relevant to them. That said, this is also a limitation that will be addressed further.

Table 1 presents the demographic characteristics of the sample.

Table 1. Demographic characteristics of the sample (N=245)

	Variable	N	Percentage %
Gender	Male	128	52.2%
	Female	117	47.8%
Age	18-22	106	43.3%
	23-29	104	42.4%
	30+	35	14.3%
Birthplace	Israel	209	85.3%
	Other	36	14.7%
Education	High School	166	67.8%
	Academic	79	32.2%

The research adhered to ethical guidelines set forth by the American Psychological Association (APA). Participants were assured that the questionnaire was anonymous and that the data collected would be used solely for research purposes.

RESEARCH VARIABLES AND VALIDATION METHOD

Data collection tool

The questionnaire used in the study comprised 38 items (see Appendix), organized into five distinct sections.

The first section (Part A, items 1-5) focused on demographic variables such as gender, age, birthplace, education level, and self-reported Internet proficiency. These variables have previously been linked to behaviors aimed at protecting privacy, including identity falsification (e.g., Dinev & Hart, 2005; Thelwall & Vis, 2017).

The second section (Part B, items 6-9) addressed participants' perceptions of privacy and anonymity in relation to identity falsification.

The third section (Part C, items 10-20) directly assessed the inclination towards identity falsification and the factors influencing this behavior. These questions were selected based on insights from the Graphic, Visualization, and Usability Center's (GVU) 7th WWW User Survey (Kehoe & Pitkow, 1997) and relevant literature, exploring triggers like trust in website operators (Acquisti et al., 2015; Miltgen & Smith, 2019), perceptions of unethical business practices (Punj, 2017), and motivations for retaliation against website operators (H. Li et al., 2019; Poddar et al., 2009).

The fourth section (Part D, items 21-27) focused on identifying which specific personal details are most susceptible to falsification and how the COVID-19 pandemic influenced participants' willingness to disclose such information. This part drew inspiration from studies such as Ismail (2018, as cited in Chegarova & Wang, 2019) and discussions on how pandemic-related government surveillance affects behaviors aimed at protecting privacy (e.g., Chan & Saqib, 2021).

The fifth section (Part E, items 28-38) explored participants' attitudes towards cooperating with epidemiological investigations during the COVID-19 pandemic and reasons for falsifying information during these inquiries. This section represented a novel investigation grounded in the idea that privacy concerns may lead individuals to prioritize personal privacy over societal benefits (Kim & Kwan, 2021) and reduce their willingness to share personal information (Fu et al., 2020).

Research variables

Based on the above-described questionnaire, the following research variables were defined (research questions that are addressed by specific variables and statistical procedures appear in parentheses. Other variables and statistical procedures were tested for descriptive purposes):

1. Socio-demographic variables:
   - Gender – Male / Female (part A, item 1)
   - Age – varied between 18-60 (part A, item 2).
   - Birthplace – Israel / Other (part A, item 3).
   - Education – High School / Academic (part A, item 4).
   - Internet proficiency level (part A, item 5) – was measured by one indicator that examined the participants' self-reported proficiency in the use of computers and the Internet. The participants' responses were recorded using a Likert scale with ratings ranging from 1 to 5 (5 – very high level of proficiency, 1 – not proficient at all).

   The differences between the socio-demographic sub-groups with regard to the dependent variable (tendency for identity falsification) were examined by a series of t-tests and ANOVA.
2. Anonymity and privacy-related issues:
   - Sense of anonymity while visiting a website (part B, item 6) – was measured by one indicator that examined the sense of anonymity while visiting a website. The participants' responses were recorded using a Likert scale with ratings ranging from 1 to 5 (5 – very high sense of anonymity, 1 – no sense of anonymity at all).
   - Sense of exposure to other users online (part B, item 7) – was measured by one indicator that examined the level of exposure to other users while surfing the web. The responses were coded on a 1-5 Likert scale (5 – not exposed at all, 1 – completely exposed).

   The two variables above were initially designed to be unified into one variable measuring online anonymity level, however, a Pearson correlation test between them was found weak ($r=0.38$) and thus suggesting two separate variables.
   - The level of privacy concern (part B, item 8) – was measured by one indicator that examined the participants' level of concern for the protection of their information online. The participants' responses were recorded using a Likert scale with ratings ranging from 1 to 5 (5 – very high level of concern, 1 – not concerned at all).

- The negative COVID-19 effect on privacy concern (**RQ4**) (part B, item 9) – was measured by one indicator that examined the level of negative change of the COVID-19 pandemic on privacy concern. The participants' responses were recorded using a Likert scale with ratings ranging from 1 to 5 (5 – very highly changed – more concerned, 1 – not changed at all).

3. Identity falsification:
   - Tendency for identity falsification (part C, item 10) – was measured by one indicator that examined the participants' level of tendency to falsify their details upon website registration. The participants' responses were recorded using a Likert scale with ratings ranging from 1 to 5 (5 – very often, 1 – never falsified personal details).
   - Factors for identity falsification (part C, items 11-20) – only for participants who had previously indicated a tendency to falsify their details (Likert scale: 2-5, N=195). These individuals were presented with 10 potential motivations for such behavior and asked to evaluate each one based on its perceived influence. Each response was coded separately on a 1-5 Likert scale (5 – very high level of influence, 1 – no influence at all):
     1) Time-consuming registration (TIME).
     2) Lack of trust in the website operators (DIST).
     3) Opaque data usage policies (TRAN).
     4) Perceived risk outweighs benefits (DISC).
     5) Concern about data dissemination to third parties (CONC).
     6) Preference for anonymity (ANON).
     7) Fear of receiving unwanted email messages (SPAM).
     8) Desire to retaliate against website operators (RVNG).
     9) Playful or mischievous intentions (TOMF).
     10) Laziness (LAZY).
4. Exposure of personal details:
   - Personal details prone to falsification (part D, items 21-26) – the participants were given six personal details and were asked to rank them by the level of reluctance to provide those details upon website registration. Each response was coded separately on a 1-5 Likert scale (5 – very high level of reluctance, 1 – not reluctant at all):
     1) Name.
     2) Address.
     3) Phone number.
     4) Identity number.
     5) Email address.
     6) Link to personal social media page.
   - The negative COVID-19 effect on the exposure of personal details (part D, item 27) – was measured by one indicator that examined the level of negative change of the COVID-19 pandemic on the willingness to expose personal details. The participants' responses were recorded using a Likert scale with ratings ranging from 1 to 5 (5 – very highly changed – lower willingness, 1 – not changed at all).
5. Epidemiological investigations:
   - Compliance with epidemiological investigations (part E, item 28) – was measured by one binary indicator. Responses were coded with the values 0 = no, 1 = yes.
   - Factors for non-compliance with epidemiological investigations (part E, items 29-38) - the participants were given ten reasons for the tendency of non-compliance with epidemiological investigations and were asked to rank them by their level of influence on this tendency. Note, that only participants who admitted to not fully complying with epidemiological investigations in the previous item (answered "no") were considered (N=5). Each response was coded separately on a 1-5 Likert scale (5 – very high level of influence, 1 – no influence at all):

1) Time-consuming registration (TIME).
2) Lack of trust in the website operators (DIST).
3) Opaque data usage policies (TRAN).
4) Perceived risk outweighs benefits (DISC).
5) Concern about data dissemination to third parties (CONC).
6) Preference for anonymity (ANON).
7) Fear of receiving unwanted email messages (SPAM).
8) Desire to retaliate against website operators (RVNG).
9) Playful or mischievous intentions (TOMF).
10) Laziness (LAZY).

DATA ANALYSIS

To predict the tendency of identity falsification upon website registration, a logistic regression analysis was performed, taking into account various independent variables: sense of anonymity on websites; sense of exposure to other users online; privacy concern; Internet proficiency; various demographic factors: gender, age, and education. A total of 2000 bootstrapped samples were used to check the validity of the model and generate an optimism-corrected C-statistic, which is a less biased method than others in the field, with lower absolute and mean squared errors (Harrell et al., 1996; G. C. S. Smith et al., 2014). The dependent variable was based on part C, item 11. A binary value of 0 was set – for all participants who reported to have never falsified their details or had a low tendency to falsify their details upon website registration (Likert scale value: 1-2); and 1 – for all participants who reported to have at least moderate tendency to falsify their details (Likert scale value: 3-5).

RESULTS

The findings show low-medium levels of the tendency for identity falsification upon website registration (M=2.45, SD=1.13), with only 19% reporting a high or very high tendency to falsify their details. As for socio-demographic differences regarding the tendency for identity falsification upon website registration, significant differences were found between men (M=2.66, SD=1.16) and women (M=2.22, SD=1.05), with men having a higher tendency to falsify their details, compared to women ($t(243)=3.12$, $p=0.002$).

RQ1a*. What are the main factors for online identity falsification?*

RQ1b*. What types of personal details are most prone to falsification?*

The study analyzed various motivations for withholding or falsifying personal information during website registration. The findings revealed that lack of trust in the website operators was the most common reason (M=3.79, SD=0.96 closely followed by the preference for anonymity (M=3.70, SD=1.20). A Cochran's Q test showed significant differences among the proposed reasons, $\chi^2(9)=601.37$, $p<0.001$, with concerns about data dissemination to third parties and lack of trust in the website operators having the highest percentage of agreement (most prevalent reasons for falsification). Figure 1 presents the mean distribution of the suggested reasons. Figure 2 presents the percentage of agreement with each of the suggested reasons. Regarding specific types of personal information, participants were most reluctant to provide their ID number (M=4.36, SD=1.08), address (M=3.97, SD=1.01), and phone number (M=3.93, SD=1.08). They were least hesitant to share a genuine link to their personal social media (M=3.50, SD=1.35), email address (M=3.09, SD=1.19), and real name (M=2.43, SD=1.09). A Cochran's Q test indicated significant differences among these personal details, $\chi^2(5)=280.90$, $p<0.001$, with ID number having the highest percentage of agreement (highest rate of falsification).

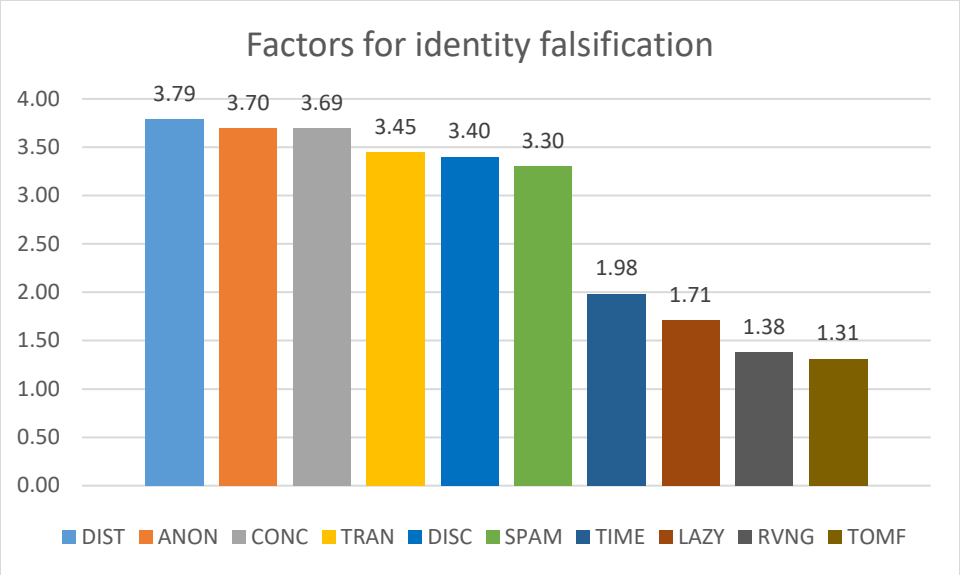

Figure 1. Mean distribution of the reasons for non-disclosure of personal details or identity falsification upon website registration.

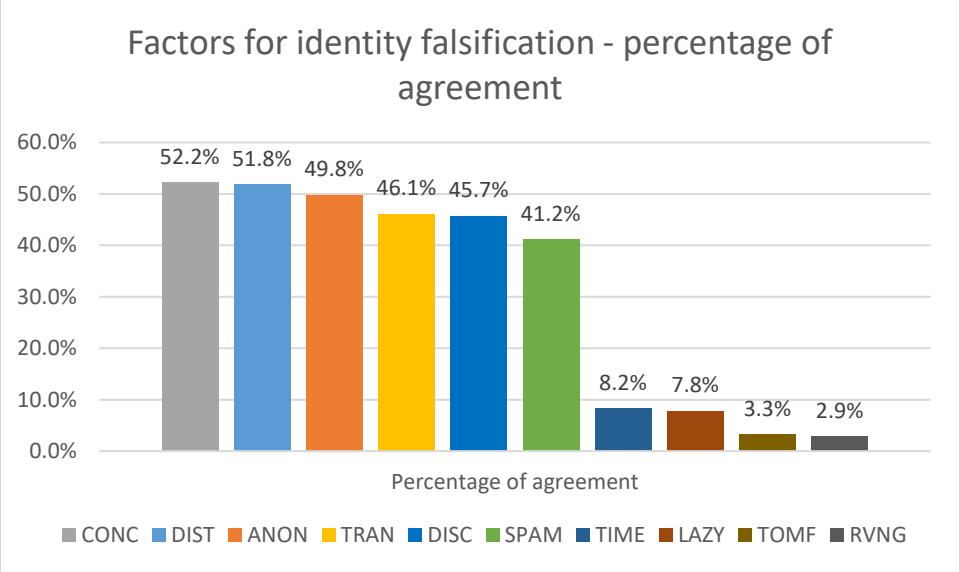

Figure 2. Percentage of agreement with each of the reasons for non-disclosure of personal details or identity falsification upon website registration.

RQ2*. Whether and to what extent do socio-demographic factors (gender, age, and education) and Internet proficiency predict the tendency for identity falsification?*

The results were also compared against socio-demographic independent variables. No significant differences were found between the socio-demographic sub-groups (gender, age, birthplace, and education). However, there were significant gender differences in the types of personal details that are prone to falsification. As women were found to be significantly more reluctant to provide their address ($t(193)=2.56$, $p=0.01$) or a link to their personal social media page ($t(193)=3.16$, $p=0.002$), compared to men.

RQ3*. Whether and to what extent do privacy-related issues, such as privacy concern and sense of online anonymity, predict the tendency for identity falsification?*

As for anonymity and privacy-related issues, the findings show medium-high levels of privacy concerns (M=3.59, SD=1.17), and low-medium sense of anonymity while visiting a website (M=2.47, SD=1.00), and a perceived sense of exposure to other users (M=2.91, SD=1.00). As for socio-demographic differences, the findings only indicate significant gender differences regarding the sense of anonymity while visiting a website (t(243)=2.80, p=0.005), as women (M=2.65, SD=1.08) had a higher sense of anonymity compared to men (M=2.30, SD=0.89).

A logistic regression analysis was conducted to predict the likelihood of users either withholding personal information or providing false identities when registering on websites. The analysis incorporated several independent variables: gender, age, education level, Internet proficiency, perceived anonymity on websites, perceived exposure to other online users, and privacy concern. Table 2 presents the regression coefficients.

Table 2. The logistic regression coefficients for the likelihood of withholding personal information or providing false identities upon website registration

Dependent variable: Likelihood for identity falsification						
					BCa 95% Confidence Interval	
Factors	B	Bias	S.E.	Exp(B)	Lower	Upper
Gender	-0.85	-0.04	0.32	**0.43****	-1.45	-0.36
Age	-0.05	-0.01	0.03	0.95	-0.12	0.003
Education	0.84	0.05	0.34	**2.32***	0.13	1.66
Internet proficiency	0.19	0.01	0.19	1.21	-0.18	0.61
Perceived anonymity on websites	0.08	0.002	0.17	1.09	-0.26	0.43
Perceived exposure to other online users	-0.13	-0.001	0.16	0.88	-0.44	0.20
Privacy concern	0.38	0.02	0.14	**1.46***	0.11	0.72

***p<0.05, **p<0.01**

The regression model yielded statistically significant results $Chi^2(7)=28.57$, $p<0.001$, with the influence variables explaining 11% (Cox and Snell $R^2=0.11$) and 15% (Nagelkerke $R^2=0.15$) of the variance. Table 2 reveals that male participants were more inclined to falsify their identities compared to females. Moreover, higher levels of education appeared to correlate with an increased tendency for identity falsification. Importantly, it was found that heightened privacy concerns positively correlated with a greater likelihood of providing false information during website registration.

RQ4. *Whether the COVID-19 pandemic affected people's privacy concerns and their willingness to share personal information, and if so, to what extent?*

Regarding the COVID-19 pandemic's impact on privacy concerns and willingness to disclose personal information, nearly two-thirds of participants (64.5%, N=245) reported increased privacy concerns. Of these, 30.6% indicated a substantial increase (scoring 4-5 on the Likert scale). Among those who admitted to falsifying their details during website registration (N=195), approximately half (49.2%) stated they became less willing to provide personal information online following the pandemic. Notably, 19.5% of this group reported being significantly less willing to do so (scoring 4-5 on the Likert scale).

RQ5. *What are the main factors not to comply with epidemiological investigations, and are they different from those of online identity falsification?*

Only 35 participants (14.3% of the sample) underwent an epidemiological investigation during the pandemic period, out of which only 5 (14.3%) admitted to not fully complying with it. The reasons for non-compliance were very similar to the ones reported for identity falsification upon website registration, as lack of transparency regarding the use of information that was collected and the participants' "private nature" were ranked as the most prevalent (M=3.40, SD=1.52). Cochran's Q test did not indicate any difference among the suggested reasons, $\chi^2(5)=12.22$, $p=0.20$.

DISCUSSION AND CONCLUSION

This research investigated the main factors for users to not disclose their personal information, or even provide falsified details upon website registration, primarily in privacy-related contexts. As privacy concerns were found to positively affect privacy-protective behavior (Sutanto et al., 2013), such as identity falsification, the research examined the influence of privacy-related variables, such as privacy concern and sense of online anonymity, on the tendency for identity falsification. The research was based on previous research (Weinberger & Bouhnik, 2019), which sought to understand users' reasons to obscure and falsify their online identities. However, as it could not fully explain this type of behavior in the past, this research examined other determinants, including social-psychological determinants, such as the desire to take revenge on the website operators. Also, it identified which personal details are most frequently falsified online. In addition, a logistic regression analysis was employed to predict the likelihood of identity falsification, considering various factors including perceived online anonymity, privacy concerns, Internet proficiency, and demographic characteristics. To add a timely perspective to the research, it explored how these issues intersect with the COVID-19 pandemic. Specifically, it examined how the pandemic influenced people's privacy concerns and their willingness to share personal information. Lastly, the research investigated whether there's a connection between individuals' reluctance to participate fully in epidemiological investigations during the COVID-19 pandemic and their tendency to provide false information online.

Although the findings showed medium-high levels of privacy concerns (M=3.59, SD=1.17), there were only low-medium levels for the tendency for identity falsification upon website registration (M=2.45, SD=1.13), with only one-fifth of the participants reporting a high or very high tendency to falsify their details. However, when it comes to the factors to falsify personal details online (**RQ1a**), privacy-related factors, such as distrust in the website operators, concern for the distribution of the information to other entities, and desire to remain anonymous, were the most prevalent for identity falsification. The social-psychological determinants (e.g., revenge or laziness) do not seem to play a large role in the decisions of whether to falsify online details. This corresponds with our previous research (Weinberger & Bouhnik, 2019) that found the desire to remain anonymous as the most prevalent reason for this behavior, and other previous studies (e.g., Acquisti et al., 2015) that suggested the issue of distrust of the website and its operators as a significant reason for the examined behavior.

An issue that was not covered in the earlier research relates to the types of personal details prone to falsification (**RQ1b**). The participants reported being most reluctant to provide their ID number (M=4.36, SD=1.08), which may be the most sensitive personal detail individuals have, as it can be used for actual identity theft. However, it seems that the participants are also very reluctant to provide their real home address (M=3.97, SD=1.01), the place where they feel the safest, and their phone number (M=3.93, SD=1.08), even more than their email address (M=3.09, SD=1.19) and name (M=2.43, SD=1.09). In addition, the relatively low rates of participants reluctant to provide a genuine link to personal social media pages (M=3.50, SD=1.35) suggest that either individuals do not comprehend the amounts of data that can be gathered from the social media (e.g., name, occupation, personal photos, etc.), or they do not care as they posted them there publicly in the first place.

As opposed to the pilot study, which could not predict the tendency for online identity falsification, this research considered additional factors in the logistic regression that was performed (**RQ2** and **RQ3**). It was found that privacy concerns significantly and positively influence the tendency for identity falsification upon website registration - the higher the privacy concern rates, the higher the chance for identity falsification. Therefore, it seems that identity falsification can be viewed as a type of privacy-protective behavior that was found in the past to be positively influenced by privacy concerns (Sutanto et al., 2013). Future research may examine this issue in the context of the personalization-privacy tradeoff and directly investigate the public stance on the equilibrium between providing genuine personal details in exchange for online benefits and maintaining personal privacy.

In addition, gender and education were found as predicting factors of the tendency for identity falsification upon website registration, as men tended more towards identity falsification compared to women. It was also found that higher education suggests a higher tendency for the examined behavior. Other examined factors, such as sense of online anonymity while visiting a website, sense of exposure to other users online, and Internet proficiency, were not found as predicting factors in this research. Interestingly, regarding the two anonymity variables (sense of online anonymity while visiting a website and sense of exposure to other users online), they were found to be weakly correlated with each other ($r=0.38$). This suggests that there is a perceived difference among the participants between anonymity vis-à-vis the visited website and other online users. It will be interesting to further explore this issue as part of future research.

As for the effect of the COVID-19 pandemic on privacy concern and the willingness to expose personal details (**RQ4**), most of the participants reported it changed their privacy concern levels for the worse (more concerned), and about half of them reported they are less willing to provide personal details over the Internet. Therefore, it seems that actions of mitigation conducted by the governments in ways that prioritized lifesaving over privacy preservation (Smidt & Jokonya, 2021), indeed increased privacy concerns among the citizens and may have influenced their online behavior. These results are a bit surprising, due to the relative apathy that Israeli citizens showed towards COVID-19-related government surveillance in the past (Duke, 2021).

One of the mitigation methods applied by the government was epidemiological investigations, which required the compliance of the participants to provide personal details. Therefore, the research tried to draw a line between the tendency not to comply with epidemiological investigations during the COVID-19 pandemic and the tendency for online identity falsification (**RQ5**). However, as the initial sample of participants who underwent an epidemiological investigation during the pandemic period was very small, it can only be assumed that the reasons for these two behaviors are very similar. A larger sample should be applied to verify these findings.

In general, it seems that privacy concerns play a significant role in moderating the tendency to falsify personal details online. Identity falsification is applied as a defensive mechanism to protect personal privacy. This corresponds with previous research that found most users are concerned with threats to their online privacy and are willing to take action to protect it (Paine et al., 2007; Wills & Zeljkovic, 2011). In addition, this trend is expected to grow even further as a result of the COVID-19 pandemic, which increased privacy concerns among online users. Therefore, website operators and online marketers should increase their transparency regarding the use of the information being collected to increase the trust among users and to eliminate privacy concerns. This will help them maintain good customer relationships, which may benefit them in the long run, as well as the consumers. In addition, local governments and internet regulators should formulate adequate laws and binding guidelines to force website operators and online marketers to take the aforementioned steps to reduce privacy concerns among internet consumers.

Finally, since the results were based on students' self-reports on their concerns and beliefs, which might be biased, future work should apply qualitative analysis to explore additional types of factors affecting online identity falsification behavior. Also, the results are limited by the relatively small

study population and reflect only Israeli students' behavior patterns, which may be biased due to their relatively higher digital proficiency. The focus on a sample population from a specific region (Israel) might also impact the findings' applicability to international audiences, since the Israeli people may be more adapted to stressful situations, and thus, it might be more difficult to assess their privacy concerns compared to other nations. In addition, due to the relatively low levels of the explained variance of both regressions, it is assumed there are other factors for predicting these behaviors that were not examined in this paper and are subject to further research. Therefore, further investigation aiming to generalize the study findings should apply the proposed methodology to additional population types, in various age groups, cultures, and countries of origin.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In G. Danezis & P. Golle (Eds), *Privacy enhancing technologies. PET 2006. Lecture notes in computer science* (pp. 36-58). Springer. https://doi.org/10.1007/11957454_3

Adams, J. S. (1963). Towards an understanding of inequity. *Journal of Abnormal and Social Psychology, 67*(5), 422-436. https://doi.org/10.1037/h0040968

Ahn, N. Y., Park, J. E., & Hong, P. C. (2020). Balancing personal privacy and public safety during COVID-19: The case of South Korea. *IEEE Access, 8*, 171325-171333. https://doi.org/10.1109/ACCESS.2020.3025971

Altman, M., Wood, A., O'Brien, D. R., & Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law, 8*(1), 29-51. https://doi.org/10.1093/idpl/ipx027

Amit, M., Kimhi, H., Bader, T., Chen, J. C., Glassberg, E., & Benov, A. (2020). Mass-surveillance technologies to fight coronavirus spread: The case of Israel. *Nature Medicine, 26*(8), 1167-1169. https://doi.org/10.1038/s41591-020-0927-z

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13-28. https://doi.org/10.2307/25148715

Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services, 52,* 101947. https://doi.org/10.1016/j.jretconser.2019.101947

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management, 53*(1), 1-21. https://doi.org/10.1016/j.im.2015.08.001

Bouhnik, D., & Deshen, M. (2014). Unethical behavior of youth in the Internet environment. *The International Journal of Technology, Knowledge, and Society,* 9(2), 109-124. https://doi.org/10.18848/1832-3669/CGP/v09i02/56372

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior, 119*, Article 106718. https://doi.org/10.1016/j.chb.2021.106718

Chegarova, V., & Wang, L. (2019). Falsifying personal data to address online privacy issues. *Issues in Information Systems, 20*(2), 183-194. http://iacis.org/iis/2019/2_iis_2019_183-194.pdf

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology & Management, 6*(2-3), 181-202. https://doi.org/10.1007/s10799-005-5879-y

Chen, R., Fang, F., Norton, T., McDonald, A. M., & Sadeh, N. (2021). Fighting the fog: Evaluating the clarity of privacy disclosures in the age of CCPA. *WPES '21: Proceedings of the 20th Workshop on Workshop on Privacy*

in the Electronic Society (pp. 73-102). Association for Computing Machinery. https://doi.org/10.1145/3463676.3485601

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change, 161*, 120299. https://doi.org/10.1016/j.techfore.2020.120299

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal 23*(5), 401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x

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. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29. https://doi.org/10.2753/JEC1086-4415100201

Duke, S. A. (2021). Nontargets: Understanding the apathy towards the Israeli security agency's Covid-19 surveillance. *Surveillance & Society, 19*(1), 114–129. https://doi.org/10.24908/ss.v19i1.14271

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160. https://doi.org/10.1016/j.chb.2008.08.006

Fox, S., Lee, R., Horrigan, J., Lenhart, A., Tom, S., & Carter, C. (2000). Trust and privacy online: Why do Americans want to rewrite the rules. *Pew Research Center's Internet & American Life Project, August 2000.* http://www.pewinternet.org/2000/08/20/trust-and-privacy-online/

French, P. E. (2011). Enhancing the legitimacy of local government pandemic influenza planning through transparency and public engagement. *Public Administration Review, 71*(2), 253-264. https://doi.org/10.1111/j.1540-6210.2011.02336.x

Fu, Y., Ma, W. H., & Wu, J. J. (2020). Fostering voluntary compliance in the COVID-19 pandemic: An analytical framework of information disclosure. *American Review of Public Administration, 50*(6-7), 685-691. https://doi.org/10.1177/0275074020942105

Harrell, F. E., Jr., Lee, K. L., & Mark, D. B. (1996). Multivariable prognostic models: Issues in developing models, evaluating assumptions and adequacy, and measuring and reducing errors. *Statistics in Medicine, 15*(4), 361-387. https://doi.org/10.1002/(sici)1097-0258(19960229)15:4%3C361::aid-sim168%3E3.0.co;2-4

Ioannou, A., I., & Tussyadiah, I. (2021). Privacy and surveillance attitudes during health crises: Acceptance of surveillance and privacy protection behaviours. *Technology in Society, 67*, 101774. https://doi.org/10.1016/j.techsoc.2021.101774

Jung, G., Lee, H., Kim, A., & Lee, U. (2020). Too much information: Assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea. *Frontiers in Public Health, 8,* Article 305. https://doi.org/10.3389/fpubh.2020.00305

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: An empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402. https://doi.org/10.1057/ejis.2008.29

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems, 34*(2), 369-400. https://doi.org/10.1080/07421222.2017.1334467

Kehoe, C., & Pitkow, J. (1997). *Graphic, Visualization, & Usability Center's (GVU) 7th WW User Survey.* https://sites.cc.gatech.edu/gvu/user_surveys/survey-1997-04/

Kim, J., & Kwan, M. P. (2021). An examination of people's privacy concerns, perceptions of social benefits, and acceptance of COVID-19 mitigation measures that harness location information: A comparative study of the US and South Korea. *ISPRS International Journal of Geo-Information, 10*(1), Article 25. https://doi.org/10.3390/ijgi10010025

Li, H., Vincent, N., Tsai, J., Kaye, J., & Hecht, B. (2019). How do people change their technology use in protest?: Understanding "protest users". *Proceedings of the ACM on Human-Computer Interaction*, Article 87. https://doi.org/10.1145/3359189

Li, Y., Rho, E. H. R., & Kobsa, A. (2022). Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites. *Behaviour & Information Technology, 41*(3), 655-677. https://doi.org/10.1080/0144929X.2020.1831608

Malheiros, M., Preibusch, S., & Sasse, M. A. (2013). "Fairly Truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In M. Huth, N. Asokan, S. Čapkun, I. Flechais, & L. Coles-Kemp (Eds.), *Trust and trustworthy computing. Trust 2013. Lecture notes in computer science* (pp. 250-266). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-38908-5_19

Miltgen, C. L., & Smith, H. J. (2019). Falsifying and withholding: Exploring individuals' contextual privacy-related decision-making. *Information & Management, 56*(5), 696-717. https://doi.org/10.1016/j.im.2018.11.004

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32-48. https://doi.org/10.1162/DAED_a_00113

Paine, C., Reips, U.-D., Steiger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of "privacy concerns" and "privacy actions". *International Journal of Human-Computer Studies, 65*(6), 526-536. https://doi.org/10.1016/j.ijhcs.2006.12.001

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215 -236. https://doi.org/10.1177/0093650211418338

Perdereaux-Weekes, A. W. (2021). *To investigate the impact of data privacy regulation on disclosure decisions: Examining consumers' willingness to share or withhold personal identifiable information in the wake of GDPR, CCPA, and LGDP* [Doctoral dissertation, St. Thomas University]. ProQuest Dissertations and Theses database.

Poddar, A., Mosteller, J., & Ellen, P. S. (2009). Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs, 43*(3), 419-448. https://doi.org/10.1111/j.1745 -6606.2009.01147.x

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems, 19*(2), 181–195. https://doi.org/10.1057/ejis.2010.15

Punj, G. (2017). Consumer intentions to falsify personal information online: Unethical or justifiable? *Journal of Marketing Management, 33*(15-16), 1402-1412. https://doi.org/10.1080/0267257X.2017.1348011

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. *Pew Research Center's Internet & American Life Project, September 2013.* https://www.pewresearch.org/internet/files/oldmedia/Files/Reports/2013/PIP_Anonym ityOnline_090513.pdf

Sannon, S., Bazarova, N. N., & Cosley, D. (2018). Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts. Paper presented at the *2018 CHI Conference on Human Factors in Computing Systems*, Montreal, QC, Canada. https://doi.org/10.1145/3173574.3173626

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *Information Society, 18*(1), 21-32. https://doi.org/10.1080/01972240252818207

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73. https://doi.org/10.1509/jppm.19.1.62.169

Sheng, H., Nah, F., & Siau, K. (2008). An experimental study in U-commerce adoption: The impact of personalization and privacy concerns. *Journal of Associations for Information Systems, 9*(6), 344 -376. https://doi.org/10.17705/1jais.00161

Smidt, H. J., & Jokonya, O. (2021). The challenge of privacy and security when using technology to track people in times of COVID-19 pandemic. *Procedia Computer Science, 181*, 1018-1026. https://doi.org/10.1016/j.procs.2021.01.281

Smith, G. C. S., Seaman, S. R., Wood, A. M., Royston, O., & White, I. R. (2014). Correcting for optimistic prediction in small data sets. *American Journal of Epidemiology, 180*(3), 318-324. https://doi.org/10.1093/aje/kwu140

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

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

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on Smartphone users. *MIS Quarterly*, 37(4), 1141-1164. https://doi.org/10.25300/misq/2013/37.4.07

Thelwall, M., & Vis, F. (2017). Gender and image sharing on Facebook, Twitter, Instagram, Snapchat and WhatsApp in the UK Hobbying alone or filtering for friends? *Aslib Journal of Information Management,* 69(6), 702-720. https://doi.org/10.1108/AJIM-04-2017-0098

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 S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp.333-365). Springer. https://doi.org/10.1007/978-94-017-9385-8_14

Weinberger, M., & Bouhnik, D. (2019). The strive for preserving online anonymity as a trigger for online identity falsification. *Journal on Systemics, Cybernetics and Informatics, 17*(2), 22-24. http://www.iiisci.org/journal/CV$/sci/pdfs/HB068AU19.pdf

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science, 1*, 1-18. https://doi.org/10.1515/opis-2017-0002

Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management and Computer Security, 19*(1), 53-73. https://doi.org/10.1108/09685221111115863

Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concern. *Journal of Service Research, 12*(2), 190–207. https://doi.org/10.1177/1094670509335772

Xing, Y. F., Li, Y. H., & Wang, F.-K. (2021). How privacy concerns and cultural differences affect public opinion during the COVID-19 pandemic: A case study. *Aslib Journal of Information Management, 73*(4), 517-542. https://doi.org/10.1108/AJIM-07-2020-0216

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *Cyberpsychology & Behavior, 11*(5), 615-617. https://doi.org/10.1089/cpb.2007.0208

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management, 56*(4), 570-601. https://doi.org/10.1016/j.im.2018.10.001

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. https://doi.org/10.1016/j.jbusres.2020.02.006

Zhang, J. H., Koivumäki, T., & Chalmers, D. (2024). Privacy vs convenience: Understanding intention-behavior divergence post-GDPR. *Computers in Human Behavior, 160*, 108382. https://doi.org/10.1016/j.chb.2024.108382

APPENDIX – ONLINE WEBSITE REGISTRATION HABITS QUESTIONNAIRE

Part A – Demographic Details

1. Sex: M / F
2. Year of birth.
3. Country of birth.
4. Education:
    1) High school.
    2) Bachelor's degree (B.A.)
    3) Master's degree (M.A.)
    4) Doctor of Philosophy (PhD)
5. How would you describe your level of Internet/computer proficiency?
    1) Not proficient at all.
    2) Low proficiency.
    3) Average proficiency.
    4) High proficiency.
    5) Very high proficiency.

Part B – Anonymity and privacy-related issues

6. How anonymous do you feel while visiting a website?
    1) Not anonymous at all.
    2) Partially anonymous.
    3) Moderately anonymous.
    4) Highly anonymous.
    5) Very highly anonymous.
7. In your opinion, how exposed are you to other users on the Internet?
    1) Completely exposed.
    2) Highly exposed.
    3) Moderately exposed.
    4) Lowly exposed.
    5) Not exposed at all.
8. How concerned are you about the protection of your personal information on the web?
    1) Not concerned at all.
    2) Slightly concerned.
    3) Moderately concerned.
    4) Highly concerned.
    5) Very highly concerned.
9. To what extent did the COVID-19 pandemic change your concern for your personal information on the web for the worse? (You are more concerned)
    1) Not changed at all.
    2) Slightly changed.
    3) Moderately changed.
    4) Highly changed.
    5) Very highly changed.

Part C – Identity falsification

10. In many websites the user is required to deliver personal details (e.g., name, phone number, email address, etc.) in order to receive various services that the website offers (website registration). In what frequency do you tend to falsify your details upon website registration?
    1) Never.
    2) Seldom.
    3) Sometimes.
    4) Often.
    5) Very often.
11. **Only for participants who did not answer "a":** To what level is the falsification done due to the following reasons? The possible answers for every reason separately were on the 1-5 Likert scale: 1) Not at all. 2) Low level. 3) Moderate level. 4) High level. 5) Very high level:

    1) Time-consuming registration (TIME).
    2) Lack of trust in the website operators (DIST).
    3) Opaque data usage policies (TRAN).
    4) Perceived risk outweighs benefits (DISC).
    5) Concern about data dissemination to third parties (CONC).
    6) Preference for anonymity (ANON).
    7) Fear of receiving unwanted email messages (SPAM).
    8) Desire to retaliate against website operators (RVNG).
    9) Playful or mischievous intentions (TOMF).
    10) Laziness (LAZY).

Part D – Exposure of personal details

12. How reluctant will you be to provide the following details? The possible answers for every reason separately were on the 1-5 Likert scale: 1) Not reluctant at all. 2) Low level of reluctance. 3) Moderate level of reluctance. 4) High level of reluctance. 5) Very high level of reluctance:

    1) Name.
    2) Address.
    3) Phone number.
    4) Identity number.
    5) Email address.
    6) Link to personal social media page.
13. To what extent did the COVID-19 pandemic change your view regarding the exposure of personal details online for the worse? (You are less willing to provide details)
    6) Not changed at all.
    7) Slightly changed.
    8) Moderately changed.
    9) Highly changed.
    10) Very highly changed.

Part E – Epidemiological investigations

14. During the COVID-19 pandemic period, did you undergo an epidemiological investigation by a representative of the Ministry of Health? Yes/No
15. **Only for participants who did not answer "No":** Did you provide all the requested details and fully cooperated with the investigation? Yes/No
16. **Only for participants who did not answer "Yes":** To what level was the falsification done due to the following reasons? The possible answers for every reason separately were on the 1-5 Likert scale: 1) Not at all. 2) Low level. 3) Moderate level. 4) High level. 5) Very high level:

    1) Time-consuming registration (TIME).
    2) Lack of trust in the website operators (DIST).
    3) Opaque data usage policies (TRAN).
    4) Perceived risk outweighs benefits (DISC).
    5) Concern about data dissemination to third parties (CONC).
    6) Preference for anonymity (ANON).
    7) Fear of receiving unwanted email messages (SPAM).
    8) Desire to retaliate against website operators (RVNG).
    9) Playful or mischievous intentions (TOMF).
    10) Laziness (LAZY).

AUTHORS

Dr. Maor Weinberger has a PhD in Information Science from Bar-Ilan University (BIU), Israel. His professional interests include online privacy and anonymity, and information security.

Prof. Dan Bouhnik is the rector of the Jerusalem College of Technology (JCT) and a former lecturer in the Information Science department at Bar-Ilan University (BIU) in Israel. He taught Computer Science and Logic in High Schools both in Israel and the United States. In addition, he is the author of a number of books used for teaching Advanced Computer Sciences in High Schools and his professional interests include virtual learning and its effect on the thinking process.