Factors for Online Identity Falsification among Israeli Students in the Era of COVID-19

Maor Weinberger
Bar-Ilan University, Israel
maor89@gmail.com

Dan Bouhnik
Jerusalem College of Technology, Israel
bouhnik@g.jct.ac.il

ABSTRACT
This research investigates the main factors which motivate users to provide falsified details upon website registration, and identifies the types of personal details that are most prone for falsification. In addition, we predict the tendency for identity falsification by examining various factors, such as: privacy concern and socio-demographic factors. We also relate those issues to the contemporaneous COVID-19 pandemic and examine its influence on privacy concerns and the willingness to expose personal details. To this end, a user study was carried out among 245 students of the Israeli academia, via a quantitative method using online closed-ended questionnaires. We found that privacy-related factors are the most prevalent for identity falsification. In addition, the regression showed the higher the privacy concerns rates, the higher chance for identity falsification. It seems that the COVID-19 pandemic increased privacy concerns among online users, which may even increase the tendency of the examined behavior.

KEYWORDS
Identity falsification; privacy concern; self-disclosure; online anonymity.

INTRODUCTION
When faced with a request for personal information, the user has three choices: disclose the information, withhold the information, or provide false information (Miltgen & Smith, 2019). Evidence suggests that many users choose to deliberately falsify information during online exchanges (Fox et al., 2000). This might occur when the users feel a loss of control over their personal information (Hoffman et al., 1999) and that it is being threatened by external parties (Sheehan & Hoy, 1999). Other factors may influence the tendency not to disclose personal details or provide falsified information upon website request include: prior experience (Poddar et al., 2009), level of trust in the website and its operators (Acquisti et al., 2015; Metzger, 2006; Miltgen & Smith, 2019), defensive reaction to perceived unethical conduct by companies (Punj, 2017), or even willingness to protest and take revenge on the website operators (Li et al., 2019; Poddar et al., 2009). In addition, the COVID-19 pandemic which erupted in December 2019 changed the approach towards privacy (Ahn et al., 2020; Kim & Kwan, 2021; Smidt & Jokonya, 2021). While public compliance was found to be vital in the successful containment of pandemics (French, 2011), as the information gathered becomes more sensitive it raises privacy concerns, causing individuals to be less concerned about the social benefit and the greater good (Kwan & Kim, 2021), and less willing to disclose their personal information (Fu et al., 2020).

This study aims to investigate the main reasons and triggers which prompt users to provide falsified information upon website request. We will also explore the types of personal details that are most prone for falsification. Furthermore, we will attempt to predict the tendency for identity falsification by examining various factors, such as: sense of online anonymity, privacy concern, Internet proficiency and socio-demographic factors. In addition, in order to provide a contemporaneous dimension we will relate those issues to the COVID-19 pandemic and examine its influence on privacy concerns and the willingness to expose personal details.

METHODS
This study was conducted among 245 students in the Israeli academia: (52.2%) men and (47.8%) women (age range: 18-60), via a quantitative method, using online closed-ended questionnaires that they were asked to complete during their academic courses of the 2020-21 school year. We chose this specific population group, as most students today are digitally-oriented and familiar with the online environment. Unfortunately, this might also have an effect on the obtained results and limit their generalizability. The participants were given 10 reasons for non-disclosure of personal details or identity falsification upon website registration and were asked to rank this reasons (10 items, 1-5 in a Likert scale): desire to remain anonymous; distrust of the website operators; the registration process takes too much time; concern of being spammed; the benefits of information disclosure do not outweigh the risks; lack of transparency regarding the use of information being collected; concern for the distribution of the information to other entities; desire to take revenge on the website operators for the hassle; tomfoolery; laziness. To predict the tendency of identity falsification upon website registration, a logistic regression analysis was performed, taking into

84th Annual Meeting of the Association for Information Science & Technology | Oct. 29 – Nov. 3, 2021 | Salt Lake City, UT.

account various independent variables: sense of anonymity in websites; sense of exposure to other users online; privacy concern; Internet proficiency; various demographic factors: gender, age, and education.

RESULTS

Among the reasons for identity falsification upon website registration, distrust in the website operators was ranked as the most prevalent (M=3.79, SD=0.96). The desire to remain anonymous was ranked second highest among all suggested reasons (M=3.70, SD=1.20). Cochran's Q test indicated significant differences among the suggested reasons, $\chi^2(9)=601.37$, $p<0.001$, with concern for the distribution of the information to other entities and distrust in the website operators having the highest percentage of agreement (most prevalent reasons for falsification). As for the types of personal details prone to falsification, the participants reported to be 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). Cochran's Q test indicated significant differences among the suggested personal details, $\chi^2(5)=280.90$, $p<0.001$, with ID number having the highest percentage of agreement (highest falsification rate).

The regression model was found significant $Chi^2(7)=28.57$, $p<0.001$, with the influence variables explaining 11% (Cox & Snell $R^2=0.11$) and 15% (Nagelkerke $R^2=0.15$) of the variance. As shown in Table 1 below, men tended more towards identity falsification compared to women. In addition, it seems that higher education suggests a higher tendency for identity falsification. Finally, we found evidence that privacy concerns positively influence the tendency for identity falsification upon website registration—the higher the privacy concerns rates, the higher the chance of 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
Sense of anonymity in websites	0.08	0.002	0.17	1.09	-0.26	0.43
Sense of exposure to other users online	-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**

Table 1. The logistic regression coefficients for the tendency of non-disclosure of personal details or identity falsification upon website registration.

As for the effect of the COVID-19 pandemic on privacy concern and the willingness to expose personal details, 64.5% of the participants (N=245) reported it changed their privacy concern levels for the worse (more concerned), and 30.6% reported it changed extensively (Likert scale rates: 4-5). Out of the participants who admitted to falsifying their details upon website registration (N=195), 49.2% reported that following the pandemic period they are less willing to provide personal details over the Internet, and 19.5% extensively less willing to do so (Likert scale rates: 4-5).

CONCLUSIONS

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 of the users are concerned about threats to their online privacy and are willing to take action in order to protect it (Paine et al., 2007; Wills & Zeljkovic, 2010). In addition, this trend is expected to grow even further as a result of the COVID-19 pandemic that increased privacy concerns among online users. Therefore, we call on website operators and online marketers to increase their transparency regarding the use of information being collected, in order to increase the trust among the users and eliminate privacy concerns. This will help them maintain good customer relationship, which may benefit them in the long run.

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

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

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.* Retrieved from: 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/10.1177/0275074020942102

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web. *The Information Society: An International Journal, 15*(2), 129 -139. https://doi.org/10.1080/019722499128583

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 number: 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

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on Web site trust and disclosure. *Communication Research, 33*(3), 155-179. https://doi.org/10.1177/0093650206287076

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

Paine, C., Reips, U.-D., Stieger, 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

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

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

Sheehan, K. B. & Hoy, M. G. (1999). Flaming, complaining, abstaining: How do you users respond to privacy concerns. Journal of Advertising, 28(3), 37-51. https://doi.org/10.1080/00913367.1999.10673588

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

Wills, C. E., and 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