The Strive for Preserving Online Anonymity as a Trigger for Online Identity Falsification

Maor WEINBERGER
Information Science, Bar-Ilan University
Ramat-Gan, 529002, Israel

Dan BOUHNIK
Computer Science, Jerusalem College of Technology
Jerusalem, 93721, Israel

ABSTRACT

In this exploratory study we investigate the main reasons and triggers for users to not disclose their personal details, or even to create a fake identity and provide falsified information upon website registration. In addition, we will examine the centrality of the desire to maintain online anonymity among the other antecedents of non-disclosure of personal details or identity falsification. Various reasons for non-disclosure of personal details or identity falsification were considered, such as the desire to remain anonymous.

To this end, a user study was carried out among 169 students of the Israeli academia, via a quantitative method using closed-ended questionnaires. The desire to remain anonymous was found as the most prevalent reason for this behavior and was always ranked as one of the top reasons among every sub-population that was examined (e.g. men / women, Bachelor / Master students, etc.). In addition, we made an attempt to predict the tendency of non-disclosure of personal details or identity falsification upon website registration, by using a multiple logistic regression taking into account various privacy and anonymity related reasons, such as anonymity awareness and privacy concern. However, it was found insignificant for the factors examined.

Keywords: online anonymity; online identity; privacy concern; self-disclosure.

1. INTRODUCTION

Anonymity is the "state of being not identifiable within a set of subjects" [1]. It is one of the unique features that the Internet provides, as it presents an exclusive platform in which users are able to shape the setting in which they operate [2]. Inside this uniquely-shaped setting, users may choose not to expose their personal details, and choose an alias or a pseudonym [3]. Despite the advanced authentication mechanisms that exist now days, users can easily register to websites using a completely wrong details and generate fake accounts [4].

There may be various reasons for not revealing real personal details upon website registration, however a significant number of studies that have investigated the phenomenon of identity falsification treated privacy concerns and control over data as the most dominant reasons [5-9]. Rainie et al. [10] have described identity masking as one of the strategies users take in order to preserve their online privacy. Fox et al. [5] even described it as a "guerilla tactic" for privacy defense. As the collection and distribution of personal information have a growing commercial potential and economic value for website operators and online marketers [6]. Therefore, there is always a risk for the selling of personal information to third-parties, without the user's knowledge or consent [10], which might result in spamming, or even identity theft [11]. The Graphic, Visualization, & Usability Center's (GVU) 7th WWW User Survey revealed that approximately 40 percent of the respondents provided false information upon website registration, while about 15 percent were found to provide falsified information over 25 percent of the time [12]. The most prevalent reason cited to resist online registration is that the website does not clearly specify the manner in which the data collected will be used. This reason was also found to be significant in later studies and was associated with the issue of trust in the website and its operators [13-16].

Another study has mentioned that identity falsification may even be driven by users' anger or willingness to take revenge on the website that hassles them with personal questions before revealing the information they seek [17].

Past research also found that consumers do not wish to reveal their true identity if it is not beneficial enough from their perspective [18-19]. However, they tend to relinquish their online privacy and anonymity, when the benefits of self-disclosure outweigh their concerns [20-24]. This type of behavior is consistent with the Uses and Gratification Theory, which claims that self-disclosing behavior occurs, due to a lack of willingness among consumers to forfeit the benefits of information disclosure, e.g. social benefits [25-26].

Other significant factors that were found to influence the intent to engage in self-disclosing behavior include: socio-demographic factors - gender and age [27-30]; users' online privacy literacy (OPL), i.e. their knowledge of the tools available to protect their information online and Internet experience [6], [26], [31], [32] and online privacy self-efficacy (OPSE), i.e. users' belief in their ability to protect their identity when surfing the Internet [33].

This study aims to investigate the main reasons and triggers for users to not disclose their personal details, or even to create a fake identity and provide falsified information upon website registration. In addition, we will examine the centrality of the desire to maintain online anonymity among the other antecedents of non-disclosure of personal details or identity falsification.

As far as we are aware, this is the first study to

comprehensively map the various factors of the deliberate creation of fake identities upon website registration and also the first to examine the place of online anonymity protection among all other factors that predict this behavior.

2. METHODS

This study was conducted among 169 students in the Israeli academia: 71 (42%) men and 98 (58%) women (age range: 18-54), via a quantitative method, using closed-ended questionnaires to complete on-site. The students were sampled from three different departments: Accounting and Business Management; Information Science; and Computer Science and Engineering.

The respondents were given eight reasons for non-disclosure of personal details or identity falsification upon website registration and were asked to rank this reasons (8 items, 1-5 in a Likert scale): desire to remain anonymous (ANON); distrust of the website operators (DIST); the registration process takes too much time (TIME); concern of being spammed (SPAM); the benefits of information disclosure do not outweigh the risks (DISC); lack of transparency regarding the use of information being collected (TRAN); lack of knowledge of website operators (KNOW); concern for the distribution of the information to other entities (CONC).
The results were also compared against socio-demographic independent variables, such as: gender, degree, field of study and also by online literacy level (three groups: novice, intermediate and experts).
To predict the tendency of non-disclosure of personal details or identity falsification upon website registration, a multiple logistic regression analysis was performed, taking into account various independent variables: anonymity awareness indicators; the level of concern for the protection of personal information on the Web; OPL; OPSE; online literacy level; various demographic factors: gender and field of study.

3. RESULTS

Among the reasons for non-disclosure of personal details or identity falsification upon website registration, distrust in the website operators was ranked as the most prevalent (M = 4.09). The desire to remain anonymous was ranked second highest among all suggested reasons. Figure 1 below presents the rank distribution of the suggested reasons.

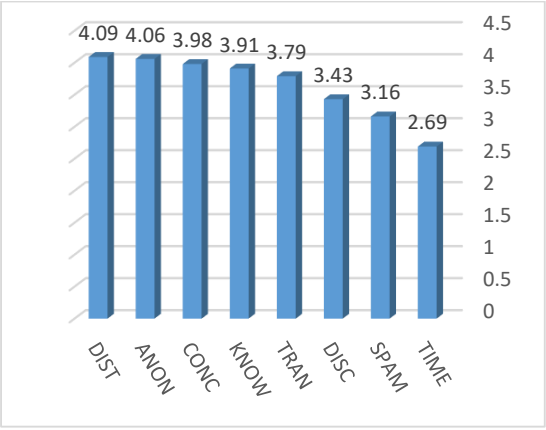

Figure 1. Rank distribution for of non-disclosure of personal details or identity falsification upon website registration

Then, we compared these results against socio-demographic independent variables. We found that the desire to remain anonymous was among the three highest ranked reasons for non-disclosure of personal details or identity falsification upon website registration, both among men (M = 4.12) and women (M = 4.02). However, this reason was ranked as the highest among men. In addition, we found differences between Bachelor and Master students regarding the ranking distribution. As Bachelor students ranked the desire to remain anonymous as the most important reason for them (M = 4.12), while Master students ranked it only as the fourth important reason (M = 3.73), while focusing on the concern for the distribution of the information to other entities (M = 4.45) and distrust of the website operators (M = 4.27).

To predict the tendency of non-disclosure of personal details or identity falsification upon website registration, a multiple logistic regression analysis was performed. However, it was found insignificant ($Chi^2(12)=14.50$, n.s., $R^2=11.6$).

4. CONCLUSIONS

This research investigated the main reasons and triggers for users to not disclose their personal details, or even to create a fake identity and provide falsified information upon website registration. In addition, we examined the centrality of the desire to maintain online anonymity among the other antecedents for non-disclosure of personal details or identity falsification. The desire to remain anonymous was found as the most prevalent reason for this behavior and was always ranked as one of the top reasons among every sub-population that was examined (e.g. men / women, Bachelor / Master students, etc.). In addition, as previous studies have suggested (e.g. [13-14, 16]), the issue of distrust of the website and its operators still remains as a significant reason for the examined behavior. However, we found no support for the Uses and Gratification hypothesis [25-26] as the reason which claims that "the benefits of information disclosure do not outweigh the risks" was one of the lowest ranked reasons among the respondents.
The differences between Bachelor and Master students regarding the placement of this reason among the others, might be explained by social and psychological characteristics. Perhaps the desire to remain anonymous is an oversimplified reason or might even be considered as childish or immature. Thus, the more matured respondents preferred to choose more "serious" reasons, such as concern for the distribution of the information to other entities and distrust of the website operators.
In addition, we made an attempt to predict the tendency of non-disclosure of personal details or identity falsification upon website registration, by using a multiple logistic regression taking into account various privacy and anonymity related reasons, such as anonymity awareness and privacy concern. However, the insignificance of the regression might suggest on other factors that predicts this variable and unfortunately were not examined in this research. These factors may be used as part of future research. Furthermore, future research may apply a qualitative phase in the form of interviews, to gain a more complete perspective of the subject matter.

5. REFERENCES

[1] Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity - a proposal for terminology. In the proceedings of*: the International Workshop on Design Issues in Anonymity and Unobservability*, H. Federrath (Ed.), pp. 1-9. Berlin, Heidelberg: Springer-Verlag.

[2] Mayer, J. R. (2009). *"Any person... a pamphleteer:" Internet anonymity in the age of Web 2.0.* Undergraduate Senior Thesis, Princeton University, Princeton, NJ.

[3] Qian, H., & Scott, C. R. (2007). Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication*, 12 (4), 1428-1451.

[4] Squicciarini, A. C., Griffin, C., & Sundareswaran, S. (2011). Towards a game theoretical model for identity

validation in social network sites. In the proceedings of: *2011 IEEE Third International Conference on Privacy, Security. Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom)*, Boston, MA.

[5] 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/

[6] Dinev, T., Xu, H., & Smith, H. J. (2009). Information privacy values, beliefs and attitudes: An empirical analysis of Web 2.0 privacy. In the proceedings of: *the 42nd Hawaii International Conference on System Sciences (HICSS '09)*, Hawaii, HI.

[7] 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.

[8] Nagle, F., & Singh, L. (2009). Can friends be trusted? Exploring privacy in online social networks. In the proceedings of: *2009 International Conference on Advances in Social Network Analysis and Mining*, Athens, Greece.

[9] Poddar, A., Mosteller, J., & Ellen, P. S. (2009). Consumers' rules of engagement in online information exchanges. *Journal of Consumer Affairs, 43* (3), 419-448.

[10] Rainie, L., Kiesler, S., Kang, R. & Madden, M. (2013). Anonymity, privacy, and security online. *Pew Research Center's Internet & American Life Project, September 2013*. Retrieved from: http://www.pewinternet.org/files/oldmedia//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

[11] Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19* (1), 62-73.

[12] Georgia Institute of Technology (1997). *Graphic, Visualization, & Usability Center's (GVU) 7th WW User Survey*. Retrieved from: https://www.cc.gatech.edu/gvu/user_surveys/survey-1997-04/

[13] Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the Web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research, 29*, 350-353.

[14] Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347* (6221), 509-514.

[15] Costante, E., den Hartog, J., & Petkovic, M. (2012). On-line trust perception: What really matters. In the proceedings of: *the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST 2011)*, Milan, Italy.

[16] Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on Web site trust and disclosure. *Communication Research, 33* (3), 155-179.

[17] Bougie, R., Pieters, R., & Zeelenberg, M. (2003). Angry customers don't come back, they get back: The experience and behavioral implications of anger and dissatisfaction in services. *Journal of the Academy of Marketing Science, 31* (4), 377-693.

[18] Kang, R, Brown, S, & Kiesler, S. (2013). Why do people seek anonymity on the Internet? Informing Policy and design. In the proceedings of: *the SIGCHI Conference in Human Factors in Computing Systems (CHI '13)*, New York, NY.

[19] Treiblmaier, H. (2005). Antecedents of the quality of online customer information. In the proceedings of: *the 2005 International Conference on Information Quality (MIT IQ Conference)*, Cambridge, MA.

[20] 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.

[21] 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.

[22] Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71* (9), 862-877.

[23] 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.

[24] Steinfeld, N. (2015), "Trading with privacy: The price of personal information", *Online Information Review*, Vol. 39 No. 7, pp. 923-938.

[25] 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.

[26] Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., et al. (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). Netherlands: Springer.

[27] Baddeley, M. (2011). A behavioural analysis of online privacy and security. *Cambridge Working Papers in Economics (CWPE), 1147*, 1-26.

[28] Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research, 7* (2), 117-141.

[29] Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers: Perceptions of marketing information management practices. *Journal of Interactive Marketing, 13* (1), 5-24.

[30] Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15* (4), 2-17.

[31] Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40* (2), 215-236.

[32] Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science, 1*, 1-18.

[33] Chen, H. T., & Chen, W. H. (2015). Couldn't or wouldn't? The influence of privacy concerns and self - efficacy in privacy management on privacy protection. *Cyberpsychology Behavior and Social Networking, 18* (1), 13-19.