AMCIS 2025 Proceedings

Americas Conference on Information Systems (AMCIS)

August 2025

How Privacy Calculus Drives Fatigue-Induced Disclosure in Generative AI

Shirin Fereidoonian
Dalhousie University, shirin.fereidoonian@gmail.com

Colin Conrad
Dalhousie University, colin.conrad@dal.ca

Recommended Citation

Fereidoonian, Shirin and Conrad, Colin, "How Privacy Calculus Drives Fatigue-Induced Disclosure in Generative AI" (2025). *AMCIS 2025 Proceedings*. 42.
https://aisel.aisnet.org/amcis2025/sigadit/sigadit/42

How Privacy Calculus Drives Fatigue-Induced Disclosure in Generative AI

Emergent Research Forum (ERF) Paper

Shirin Fereidoonian
Dalhousie University
shirin.fereidoonian@dal.ca

Colin Conrad
Dalhousie University
colin.conrad@dal.ca

Abstract

As generative artificial intelligence (GAI) becomes increasingly prevalent, concerns regarding information disclosure have garnered considerable attention. In this research-in-progress paper, expand on existing theories of privacy disclosure by introducing eye tracking measures and an experiment which will investigate the effectiveness of an informational privacy nudging technique. We hypothesize that privacy nudges will moderate the relationship between privacy calculus and varieties of privacy fatigue. We introduce an expanded conceptual model and describe an eye tracking experiment that can validate it. This research will also offer insights into whether past models of privacy disclosure generalize in the new context of effective and safer GAI design.

Keywords

Cybersecurity fatigue, Information disclosure, Privacy, Eye tracking, Digital nudging

Introduction

Over the past two years, generative artificial intelligence (GAI) platforms, such as ChatGPT, have exploded in popularity due to their ability to generate novel content with simple prompted requests (Feuerriegel et al., 2023). While these technologies are quickly changing how we learn and work, they have recently come under increasing scrutiny from the perspective of information privacy disclosure. Regulators and scholars have raised concerns about how large language models have utilized large data repositories in their development, which could allow users to prompt these systems to re-identify previously de-identified data (Gumusel, 2025). Furthermore, unlike past technologies, GAI systems can dynamically change their requests to a user leading them to inadvertently disclose sensitive information (Feuerriegel et al., 2023).

Concerns about online privacy disclosure are not new (Furnell & Thomson, 2009). In existing systems such as mobile applications, users face the challenging task of navigating the trade-off between reaping the benefits of virtual activities and safeguarding their privacy, which is a mental process, as previous research called “privacy calculus” (Sun et al., 2015; Zhu et al., 2021). However, this delicate balance becomes even more complex in the context of privacy fatigue in GAI. When people are overwhelmed with continuous exposure to prompts related to sharing personal information, their decision-making abilities regarding privacy may become tedious (van der Schyff et al., 2023; Zhu et al., 2021).

Increasingly, companies that build GAI systems have considered such cognitive processes and have implemented persuasive designs. For example, Meta has taken steps to label AI-generated multimedia on its platforms (Bickert, 2024). This approach is one of the applications of a broader movement often referred to as “digital nudging,” through which a user is guided to positive behavior in choice environments by changing the interface design in a non-coercive way (Kroll & Stieglitz, 2021). However, there are reasons to believe that changes to an interface design actually increase information disclosure, rather than decrease it, due to the nudge design's increased fatigue effects. These effects, sometimes referred to as “privacy fatigue” are the varieties of exhaustion that individuals face when confronted with repeated privacy requests, which may be either cognitive or attitudinal in nature (Choi et al., 2018; Tian et al., 2022).

In this paper, we propose a study investigating the role of varieties of privacy fatigue, whether attitudinal or physical, and the moderating role of privacy nudging. This model will be used to investigate disclosure using a GAI platform modeled on Open AI's ChatGPT. Our study makes two main contributions. First, we use eye tracking as a physical measure of cognitive privacy fatigue. Cognitive varieties of fatigue or mental workload are often unreliably assessed by users, and capturing hidden mental processes is one of the central contributions of neurophysiological approaches to information systems (or “NeuroIS”) research (Riedl & Léger, 2016). Second, we extend the prior research on this topic which has been overwhelmingly focused on mobile applications (Tian et al., 2022; Zhu et al., 2021), though now also increasingly in the domain of GAI (Chung & Kwon, 2025) to the use of the privacy nudging technique. This short paper will describe our conceptual model and an experiment for testing it.

Literature Review and Hypothesis Development

GAI is poised to become one of the most disruptive technological trends of our era, and there is pressing demand by public authorities to investigate ways that people can use it safely (Gumusel, 2025). In GAI use environments, like many other IT use environments, people constantly need to make decisions about sharing personal information. There are many approaches to studying privacy decision behavior; however, the privacy calculus remains one of the prominent approaches in that literature (Heravi et al., 2017). This concept can be summarized succinctly as a struggle between privacy risks and benefits (Zhu et al., 2021).

Researchers have hypothesized that cybersecurity fatigue, which is a fatigue created by overexposure to cybersecurity-related phenomena, plays a mediating role between the privacy calculus and disclosure behavior (Fereidoonian & Wingreen, 2024), and has been identified as relevant to disclosure when using GAI (Chung & Kwon, 2025). Reeves et al. (2021) conducted a literature review and determined that privacy fatigue has two types, cognitive and attitudinal, which are distinguished by different underlying processes. Attitudinal fatigue was described by Reeves et al. (2021) to refer to a negative disposition towards cyber security, which in other research associated with antecedents like emotional exhaustion (Sheng et al., 2023) and cynicism (Choi et al., 2018). Cognitive fatigue, by contrast, refers to the internal state of an employee or user. This is reflected by physical states such as cognitive overload, which is the experience of being overloaded by information (D’Arcy et al., 2014) or impulsivity which is the inhibition of long-term oriented, executive processes (Ostendorf et al., 2022).

One challenge with measuring cognitive states, such as cognitive overload or impulsivity, is that states can fluctuate during an experience, resulting in an unreliable personal assessment by users (Chen & Epps, 2014). This motivates us to propose a NeuroIS approach to our research, which can help objectively measure phenomena when questionnaires may not be appropriate (Riedl & Léger, 2016). Specifically, eye tracking techniques have been used to measure similar cybersecurity phenomena (Vance et al., 2018) and there are measures which directly relate to the elements of cognitive fatigue. Eye saccade velocity can reflect a user's general attentional fatigue and, in turn, cognitive overload (Bafna & Hansen, 2021; Zagermann et al., 2016). Additionally, pupil dilation has been associated with emotional states related to impulsivity (Riedl & Léger, 2016, p. 201; Zagermann et al., 2016). By studying these physiological measures, we can increase the reliability and explainability of existing information disclosure models.

A second contribution can be made by studying newer trends in persuasive design, such as digital nudging (Kroll & Stieglitz, 2021). There are growing concerns about the propensity of GAI systems to encourage user information disclosure (Gumusel, 2025), and one possible technique for encouraging safer behavior is to provide an informational nudge, such as a safety reminder (what we will call a “privacy nudge”). Privacy nudges may increase users' attention and awareness of disclosing their information, which is an approach that has been attempted by leading companies such as Meta (Acquisti et al., 2017; Bickert, 2024). By incorporating a privacy nudge in an interface design, designers can help reduce deliberative behavior and help the privacy calculus process to reduce different types of privacy fatigue. Given these considerations, we propose a conceptual model and hypotheses, which are illustrated by Figure 1. This model expands on the model originally introduced by Fereidoonian and Wingreen (2024) by introducing a refined articulation of privacy calculus as well as the privacy nudge and its effects on specific varieties of fatigue.

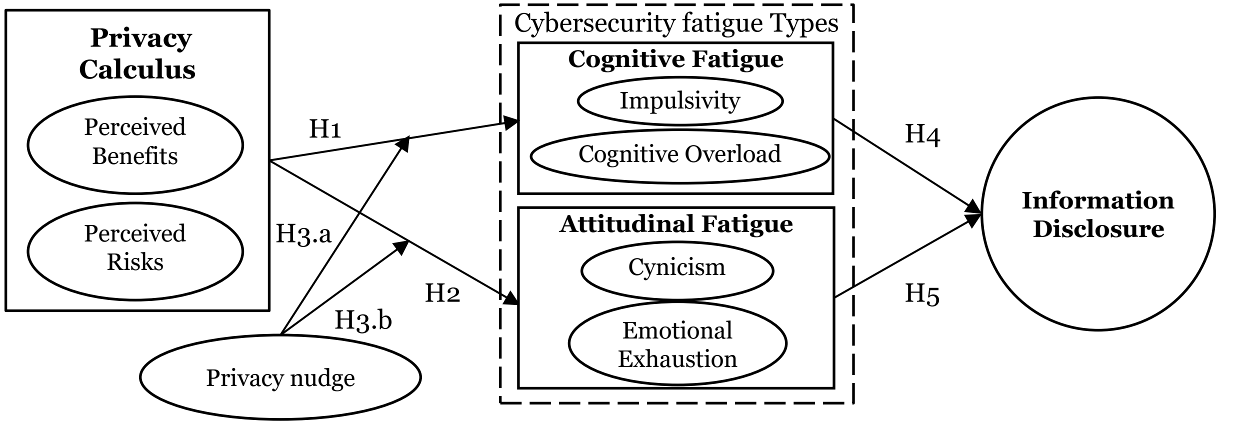

Figure 1. Proposed Conceptual Model

We hypothesize that:

H1 – Privacy calculus will positively impact cognitive fatigue.

H2 – Privacy calculus will positively impact attitudinal fatigue.

H3a – Privacy nudges weaken (negatively moderate) the relationship between net privacy calculus and cognitive fatigue.

H3b – Privacy nudges weaken (negatively moderate) the relationship between net privacy calculus and attitudinal fatigue.

H4 – Cognitive fatigue will positively impact information disclosure behavior.

H5 – Attitudinal fatigue will positively impact information disclosure behavior.

Our reasoning is that if a negative privacy calculus (i.e., the user perceives that risks outweigh benefits) typically leads to higher cybersecurity fatigue, information nudges may help users manage privacy concerns, reducing their feelings of being overwhelmed. For individuals with a positive net privacy calculus (i.e., benefits outweigh risks), nudges may reinforce their confidence, further reducing fatigue.

Experiment Design

Seventy-four participants will be recruited from the university. The number of participants was determined using G Power's Linear multiple regression test with a medium Effect size f2 measure of 0.15 and power (1 – β) of 0.95 (Faul et al., 2007). Participants will be awarded either partial course credit or financial compensation of CAD 10 for participating in the study.

After consenting, on day one, we will give students some questionnaires to fill out to test our conceptual model and make sure about the constructs and their relations. On day two, they will be brought to an observational room equipped with a computer and an eye tracker. The interface will follow a similar design to ChatGPT and be developed using the GPT-4 chat API. Participants will conduct three tasks with a virtual agent using the within-subject method, which is most appropriate for designs using eye tracking (Unsworth & Robison, 2015). The tasks are described as follows: an information-seeking task with no privacy nudge, an information-seeking task with a privacy nudge, and a control task that does not involve information-seeking. The order of these tasks will be randomized using a Latin Square Design to prevent order effects such as learning, habituation, and so forth.

For the information-seeking tasks, participants will be asked to use the assistant for advice on how to start a company with a given structure (e.g., "corporation," "partnership," "cooperative") at random. The agent will be pre-programmed with documents from our local jurisdiction with instructions on how to advise participants, as well as instructions to prompt users to provide some personal information about their name and academic background. For the control task, participants will be instructed to use the machine to generate name and location ideas for their business, and they will not be prompted to disclose personal information. In the nudging condition, participants will be reminded not to disclose personal information with a visual cue on the screen. Following each task, users will complete a questionnaire.

The measures used in this study consist of a combination of eye-tracking data and questionnaires. In addition to demographic data like (reported gender, age, educational level, and experience with GAI), we will offer 7-point Likert scales for emotional exhaustion, net privacy calculus, and cynicism (Tian et al., 2022; Zhu et al., 2021). Privacy nudges will be measured as a binary yes/no based on whether they were present during the experiment. Pupil dilation will be used to measure impulsivity and saccade velocity will be used to measure cognitive overload (Bafna & Hansen, 2021; Riedl & Léger, 2016) and will be measured using the Tobii Pro Fusion 250 Hz system with a multi-point calibration procedure before the start of each task. Hypotheses will be tested using linear mixed-effects models, as demonstrated by Vance et al. (2018), which are most appropriate for within-subject physiological designs.

Conclusion

If successful, this research will expand on current theories on privacy disclosure by offering physiological insights into cognitive fatigue and an assessment of the effectiveness of privacy nudges on ensuring AI disclosure safety. The study may pave the way for future responsible AI research on privacy fatigue, as and potentially the development of new regulations or policies for GAI.

REFERENCES

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.*, *50*(3), 44:1-44:41. https://doi.org/10.1145/3054926

Bafna, T., & Hansen, J. P. (2021). Mental fatigue measurement using eye metrics: A systematic literature review. *Psychophysiology*, *58*(6), e13828. https://doi.org/10.1111/psyp.13828

Bickert, M. (2024, April 5). Our Approach to Labeling AI-Generated Content and Manipulated Media. *Meta*. https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media/

Chen, S., & Epps, J. (2014). Using Task-Induced Pupil Diameter and Blink Rate to Infer Cognitive Load. *Human–Computer Interaction*, *29*(4), 390–413. https://doi.org/10.1080/07370024.2014.892428

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Chung, J., & Kwon, H. (2025). Privacy fatigue and its effects on ChatGPT acceptance among undergraduate students: Is privacy dead? *Education and Information Technologies*, 1–23. https://doi.org/10.1007/s10639-024-13198-6

D'Arcy, J., Herath ,Tejaswini, & and Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/BF03193146

Fereidoonian, S., & Wingreen, S. (2024). Sources and Types of Cybersecurity Fatigue: Impact on Information Disclosure. *AMCIS 2024 Proceedings*. https://aisel.aisnet.org/amcis2024/cog_res/cog_res/10

Feuerriegel, S., Hartmann, J., Janiesch, C., & Zschech, P. (2023). *Generative AI* (SSRN Scholarly Paper 4443189). https://doi.org/10.2139/ssrn.4443189

Furnell, S., & Thomson, K.-L. (2009). Recognising and addressing 'security fatigue.' *Computer Fraud & Security*, *2009*(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

Gumusel, E. (2025). A literature review of user privacy concerns in conversational chatbots: A social informatics approach: An Annual Review of Information Science and Technology (ARIST) paper. *Journal of the Association for Information Science and Technology*, *76*(1), 121–154. https://doi.org/10.1002/asi.24898

Heravi, A., Mani, D., Choo, K.-K. R., & Mubarak, S. (2017). Making Decisions about Self-Disclosure in Online Social Networks. *Hawaii International Conference on System Sciences 2017 (HICSS-50)*. https://aisel.aisnet.org/hicss-50/dsm/decision_making_in_osn/4

Kroll, T., & Stieglitz, S. (2021). Digital nudging and privacy: Improving decisions about self-disclosure in social networks. *Behaviour & Information Technology*, *40*(1), 1–19. https://doi.org/10.1080/0144929X.2019.1584644

Ostendorf, S., Meier, Y., & Brand, M. (2022). Self-disclosure on social networks: More than a rational decision-making process. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *16*(4), Article 4. https://doi.org/10.5817/CP2022-4-2

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *Sage Open*, *11*(1), 21582440211000049. https://doi.org/10.1177/21582440211000049

Riedl, R., & Léger, P.-M. (2016). *Fundamentals of NeuroIS*. Springer.

Sheng, N., Yang, C., Han, L., & Jou, M. (2023). Too much overload and concerns: Antecedents of social media fatigue and the mediating role of emotional exhaustion. *Computers in Human Behavior*, *139*, 107500. https://doi.org/10.1016/j.chb.2022.107500

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior*, *52*, 278–292. https://doi.org/10.1016/j.chb.2015.06.006

Tian, X., Chen, L., & Zhang, X. (2022). The Role of Privacy Fatigue in Privacy Paradox: A PSM and Heterogeneity Analysis. *Applied Sciences*, *12*(19), Article 19. https://doi.org/10.3390/app12199702

Unsworth, N., & Robison, M. K. (2015). Individual differences in the allocation of attention to items in working memory: Evidence from pupillometry. *Psychonomic Bulletin & Review*, *22*(3), 757–765. https://doi.org/10.3758/s13423-014-0747-6

van der Schyff, K., Foster, G., Renaud, K., & Flowerday, S. (2023). Online Privacy Fatigue: A Scoping Review and Research Agenda. *Future Internet*, *15*(5), Article 5. https://doi.org/10.3390/fi15050164

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments. *MIS Quarterly*, *42*(2), 355–380.

Zagermann, J., Pfeil, U., & Reiterer, H. (2016). Measuring Cognitive Load using Eye Tracking Technology in Visual Computing. *Proceedings of the Sixth Workshop on Beyond Time and Errors on Novel Evaluation Methods for Visualization*, 78–85. https://doi.org/10.1145/2993901.2993908

Zhu, M., Wu, C., Huang, S., Zheng, K., Young, S. D., Yan, X., & Yuan, Q. (2021). Privacy paradox in mHealth applications: An integrated elaboration likelihood model incorporating privacy calculus and privacy fatigue. *Telematics and Informatics*, *61*, 101601. https://doi.org/10.1016/j.tele.2021.101601