Association for Information Systems
AIS Electronic Library (AISeL)

ECIS 2025 Proceedings | European Conference on Information Systems (ECIS)

June 2025

ROLE OF DATA SECURITY IN DIGITAL DATA WALLETS ADOPTION: AN ELABORATION LIKELIHOOD MODEL PERSPECTIVE

Varvara Keba
Universidade NOVA de Lisboa, vkeba@novaims.unl.pt

Tiago Oliveira
NOVA Information Management School (NOVA IMS), toliveira@novaims.unl.pt

Follow this and additional works at: https://aisel.aisnet.org/ecis2025

Recommended Citation

Keba, Varvara and Oliveira, Tiago, "ROLE OF DATA SECURITY IN DIGITAL DATA WALLETS ADOPTION: AN ELABORATION LIKELIHOOD MODEL PERSPECTIVE" (2025). *ECIS 2025 Proceedings*. 6.
https://aisel.aisnet.org/ecis2025/security/security/6

This material is brought to you by the European Conference on Information Systems (ECIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2025 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

ROLE OF DATA SECURITY IN DIGITAL DATA WALLETS ADOPTION: AN ELABORATION LIKELIHOOD MODEL PERSPECTIVE

Short Paper

Varvara Keba, NOVA Information Management School, Universidade NOVA de Lisboa, vkeba@novaims.unl.pt

Tiago Oliveira, NOVA Information Management School, Universidade NOVA de Lisboa, toliveira@novaims.unl.pt

Abstract

This study examines the motivations behind adopting digital data wallets, a type of privacy-enhancing technology, and the role of data security in shaping users' attitudes toward the tool. A qualitative study employing a mixed method approach is used to identify the key motivational factors based on motivation theory. The research model was built based on the elaboration likelihood model and identified factors. The quantitative study will then test the model using data from Austria, Romania, and Spain.

Keywords: Digital data wallets, Privacy-enhancing technology, Motivation, Data security

1 Introduction

Nowadays, individuals provide extensive information online to buy products or services. As individuals increasingly use various tools and electronic services, their focus on security measures also increases. 87% of individuals mentioned that they would avoid doing business with a company if they had concerns about its security measures (Anant et al., 2020). As a result, people want to regain some control over their privacy online (Ashuri, 2024; Silva et al., 2022). Despite the availability of privacy-enhancing technologies, such as digital data wallets, the adoption of these technologies remains limited (Zou et al., 2020; European Union Agency for Cybersecurity, 2019). Hence, this study focuses on examining individual behaviour regarding the adoption of digital data wallets - a kind of privacy-enhancing technology. Digital data wallets (DDWs) are personal data management platforms that provide users with control over their personal data, enable safe storage and sharing, and minimise exposure while accessing online services (European Commission, 2023; SOTERIA, 2023). In information system (IS) literature, few studies have analysed the adoption of privacy-enhancing technologies from the potential users' perspective (Bracamonte et al., 2022; Coopamootoo, 2020). Most studies primarily concentrate on technological artefacts and solutions for managing privacy online (Harborth & Pape, 2020; Bélanger & Crossler, 2011). Some studies have examined the adoption of privacy-enhancing technologies and identified important factors, such as usability and trust. However, users still consider advanced privacy-enhancing technologies complex and challenging, highlighting the need to identify and understand individual requirements so as to improve adoption and user experience. Consequently, the motivations driving individuals' adoption of privacy-enhancing technologies, such as DDWs, remain unclear.

In technology adoption literature, security concerns are considered a significant obstacle (Oliveira et al., 2016). Additionally, one of the reasons for not using privacy-enhancing technologies and practices is the risk associated with security (Zou et al., 2020). DDWs enable users to control the information they share online. Hence, with the growing number of cyberattacks, potential users pay close attention to security measures provided by DDWs to protect their information. Therefore, the study seeks to answer the following questions:

1. What is the motivation to form an attitude toward DDWs?

2. How does data security influence motivation and attitude toward DDWs?

A mixed methods approach was adopted to answer the research questions. Firstly, a qualitative study was conducted to identify motivational factors that form an attitude toward DDWs based on the motivation theory (Deci, 1976). The research model was developed based on the qualitative study results and elaboration likelihood model (Petty & Cacioppo, 1986; Petty et al., 1981). The research model is incomplete and will be tested in the quantitative study.

The contribution of the study is threefold. Firstly, the study contributes to privacy-enhancing technology adoption literature by identifying both extrinsic and intrinsic motivations to form an attitude toward DDWs based on motivation theory. Secondly, the study enhances the theoretical perspective on data security, analysing their moderation effect based on the elaboration likelihood model. The influence of data security on motivation to adopt DDWs will be tested in a quantitative study. Finally, the study identifies individuals' motivation to adopt DDWs. The findings provide insights for DDW developers.

The remainder of the paper is organised as follows. Section 2 presents the theoretical background. The research methodology is explained in section 3. Section 4 outlines the qualitative study. The research model and hypotheses are discussed in section 5. Section 6 presents the conclusion and next steps.

2 Theoretical background

2.1 Digital data wallets and motivation

DDWs are personal data management platforms providing users with secure and convenient ways to store and share their data while accessing electronic services (European Commission, 2023; SOTERIA, 2023). This technology aims to facilitate and provide protected access to online services and inform their users about the risks associated with data sharing (SOTERIA, 2023). DDWs can be considered a kind of privacy-enhancing technology. Privacy-enhancing technologies aim to decrease the unnecessary processing of personal information by restricting information disclosure (Fischer-Hbner & Berthold, 2017). The main aim of DDWs is to provide individuals with control over their shared information online, including minimisation of the data shared with service providers (SOTERIA, 2023).

Information privacy is a form of control over the use of personal information (Bélanger & Crossler, 2011). IS literature has explored the role of privacy across various contexts, highlighting the importance of perceived control, privacy literacy, and the relationship between risks and benefits. Perceived control is a key aspect of privacy, reflecting the belief in one's ability to decide how much personal information to share online (Dinev et al., 2013). Individual privacy is growing more important, yet people may share personal information when it leads to benefits (Cheng et al., 2021). Usability and user-friendliness are considered crucial factors in the adoption of privacy-enhancing technologies. Previous studies examining the behaviour of privacy-enhancing technologies users underlined the importance of providing user-friendly applications and adapting privacy-enhancing technologies to users' preferences (Ashuri, 2024; Kaaniche et al., 2020; Coopamootoo, 2020). Additionally, trust plays an important role in adopting privacy-enhancing technologies, as it is considered a significant barrier to adoption (Harborth & Pape, 2020; Coopamootoo, 2020). Other factors, such as awareness, usefulness, need for privacy, cost, and social support, influenced the choice to use privacy-enhancing technologies (Coopamootoo, 2020). The literature found some factors influencing individuals' behaviour; nevertheless, little is known about the potential users' motivation to adopt privacy-enhancing technologies.

The motivation theory has been adopted to fill this gap. According to the motivation theory, both extrinsic and intrinsic motivations influence an individual's behavioural intention (Deci, 1976). Extrinsic motivation is when individuals perform an action due to its perceived usefulness in gaining value. Intrinsic motivation is when individuals act because of interest in the action itself. In the context of technology adoption and social commerce, perceived usefulness is often considered extrinsic motivation, and perceived enjoyment is frequently regarded as intrinsic motivation (Neves et al., 2023; Hu et al., 2022; Lin & Lu, 2011). Previous literature on privacy-enhancing technologies adoption mainly focused on extrinsic motivation, for example, identifying factors like user-friendliness and usefulness

as the main drivers that can lead to adoption (Ashuri, 2024; Coopamootoo, 2020; Harborth & Pape, 2020). Nevertheless, despite the valuable features of the technologies, intrinsic motivation can lead to higher user engagement with the technology. DDWs are innovative technology. Hence, a qualitative study is conducted in order to identify potential users' extrinsic and intrinsic motivation.

2.2 Data security and elaboration likelihood model

Security is the protection of data from unauthorised access as well as damage (Belanger et al., 2002). Privacy and security are different concepts. However, they are strongly linked with each other, as security is essential to providing a sense of privacy online (Benson et al., 2015). Cichy et al. (2021) found that drivers' beliefs about data security are closely intertwined with their privacy concerns. Hence, in the case of DDWs, individuals' perceptions of data security can significantly influence users' behaviour. While adopting privacy-enhancing technologies, individuals choose to protect their privacy online, but they may also consider the security measures provided by technology.

The elaboration likelihood model is adopted to better understand how potential users' perception of data security influences motivation and attitude toward DDWs. The elaboration likelihood model is the dual process theory concerning the formation and change of attitude subsequent to persuasion outcomes (Petty & Cacioppo, 1986; Petty et al., 1981). According to the paradigm, there are two routes for individuals' attitudes to change, specifically the central and peripherical routes, which differ based on the motivation and ability to process information (Bhattacherjee & Sanford, 2006). The central route requires individuals to think critically about the related content of an informational message, analyse it, and examine other related issues. Hence, the central route requires more cognitive effort and is persuaded by the quality of the argument. For example, in the context of information technology acceptance, the potential benefits of the system usage, the quality and availability of the system support, comparison with alternative systems, and the cost of the system acceptance could be considered arguments (Bhattacherjee & Sanford, 2006). In the context of privacy-enhancing technology adoption, it is argued that extrinsic motivation can be considered a central route because potential users are more likely to assess the perception of the usefulness of DDWs usage cognitively. The peripherical route requires less cognitive effort, which requires individuals to consider some obviously positive or negative cues, such as the number of prior users and the likeability of endorsements (Bhattacherjee & Sanford, 2006). As the adoption of privacy-enhancing technologies and practices remains low (Zou et al., 2020), it is argued that intrinsic motivation can be considered a peripheral route because potential users' intrinsic motivation can serve as a simple inference requiring less cognitive effort. Elaboration likelihood is used to establish individuals' motivation and ability to appraise the key merits of a targeted item (Kwak et al., 2018). It is argued that individuals' perception of data security is an immediate motivator in assessing extrinsic and intrinsic motivations.

3 Mixed methods design

A mixed methods approach was adopted to answer the research questions. The qualitative study answers the first research question, specifically to recognise the motivation to use DDWs. The research model is built based on the results of the qualitative study. The quantitative analysis will be used to answer the second research question, specifically to test the research model and analyse the role of data security in the context of DDWs. The quantitative study is in progress.

4 Qualitative study

Thirty interviews were conducted with individuals from Austria, Romania, and Spain. The data were collected from Central, Eastern, and Western Europe to represent the sample of the European Union. The participants were recruited using a purposive sample approach to ensure diversity in ages, genders, and digital literacy. The interviews were conducted in the participant's native language (German, Romanian, and Spanish). The interview duration ranged from 35 to 80 minutes. An interview guide with both open-ended and close-ended questions was used. First, participants were asked about their overall use of privacy-enhancing devices. Afterwards, the participants were shown the SOTERIA DDW

(SOTERIA, 2023), and interview questions were centred on what they liked and disliked about the DDW, as well as their motivation to use the technology. In order to reach data saturation, the interviews were conducted until conceptual themes began to repeat to reach data saturation (Fusch & Ness, 2015).

The theoretical engagement principle is applied to qualitative data analysis (Sarker et al., 2013). The motivation theory is used as the theoretical frame for the study. The goal is to identify extrinsic and intrinsic motivations influencing the attitude toward DDWs. An open coding methodology is followed to analyse the data, segmenting data for quotes and associating it with categories. Accordingly, a list of categories was created based on transcription. Table 1 presents representative quotations.

Categories		**Quotes**
Extrinsic motivation	Privacy control	*"I would need to be able to decide what information I give out and what not. And I would need to decide very easily what I want to give." (Interviewee 3), "I definitely like the option of giving selective information out of that digital wallet that you can really control." (Interviewee 5), "the main advantage is that you also have control over your data." (Interviewee 11).*
	Transparency	*"The more transparent the relationship between the manufacturer or developer of this platform and the person trying to use or want to use, the more willing the person is to use it." (Interviewee 18), "When you download this platform, and you register here, it has to be like as much as transparent as possible." (Interviewee 10), "But if there is any sort of sign of non-transparency within that company, I'm probably going to maybe look for an alternative." (Interviewee 8).*
Intrinsic motivation	Convenience	*"If the app were integrated with many other private services, it's possible that you might use it for convenience." (Interviewee 14), "In the end, it [DDWs] has to be comfortable; it saves time." (Interviewee 22), "It would be super comfortable instead of having so many documents around, fast access to data all the time and not having to look for the physical copies or the physical documents every time you need something." (Interviewee 10).*
	Social influence	*"If my friends or my parents or someone told me that it was very good, I would use it." (Interviewee 24), "I would for sure look for reviews and experiences of others regarding this platform. I would read more about it on the internet." (Interviewee I8), "If they [DDW providers] have very good reviews from other people, I may give it a go and try." (Interviewee 20).*

Table 1. Representative quotations.

Based on the qualitative study, extrinsic motivation factors, specifically privacy control and transparency, and intrinsic motivation factors, specifically convenience and social influence, were identified. Extrinsic motivation is to perform an action because of its perceived helpfulness in gaining value. The main goal of DDWs is to allow users to fully control their privacy online. Privacy control is a person's belief in their ability to decide how much personal information will be shared online (Dinev et al., 2013). Hence, individuals expect that the main useful feature of DDWs will be privacy control. Transparency is also considered an extrinsic motivation. Transparency is disclosing information about the types of data an organisation has collected about individuals and how that data will be used (Dinev et al., 2013). Participants expressed a clear desire for transparency. They expect DDWs to provide privacy policies and security measures and make them clear and available to users. Hence, transparency can increase the helpfulness of DDWs because the more transparent the technology is, the clearer it will be for users to understand how their personal information is treated in DDWs and the level of privacy control they have over their personal information.

Intrinsic motivation refers to performing an action because of interest in the action itself. DDWs are new technology. Hence, if DDWs are more convenient than current methods of online information sharing, this tool may attract interest from potential users. Convenience is a reduction in the time or energy necessary to use a product or service compared to the present situation (Brown & McEnally, 1992). Participants expect that DDWs will provide more flexible service than traditional information sharing while accessing electronic services. Social influence is also considered intrinsic motivation.

Social influence refers to individuals' perception of how important others, such as friends and family, believe that they have to use technology (Venkatesh et al., 2012). If the new technology, such as DDWs, is highly recommended for use by friends and family, individuals could form good perceptions of the technology. Participants mentioned that they definitely search for reviews from other users. Nevertheless, if they hear the suggestion to use DDWs from friends and family, they will probably use it.

5 Research model and hypotheses

Figure 1 presents the research model. The results of the qualitative study are implemented in the research model. Based on the motivation theory and elaboration likelihood model, extrinsic motivation is considered the central route. Privacy control and transparency were identified as extrinsic motivations in the qualitative study. Privacy control and transparency reflect the aspect of information quality in the central route because, in the context of DDWs, individuals are more likely to cognitively assess the level of privacy control that potential users have and how transparent DDWs are with their users. Hence, it is argued that privacy control and transparency will positively influence attitude.

Intrinsic motivation is considered the peripheral route. Based on the qualitative study, convenience and social influence were identified as intrinsic motivations. Convenience and social influence are considered straightforward inferences that involve little cognitive effort. Convenience makes DDWs more attractive in comparison to other information-sharing methods online, which helps to involve or persuade the potential user. Additionally, users can rely on their close-circle recommendations to form an attitude toward DDW usage. Hence, it is argued that convenience and social influence will positively influence attitude.

Data security is considered as elaboration likelihood. Not many people have previously used any kind of privacy-enhancing technology. Hence, previous data breaches that form individuals' concerns regarding data security can influence their ability to elaborate on informational messages. Thus, it is argued that data security will moderate the relationship between extrinsic motivation and attitude, as well as the relationship between intrinsic motivation and attitude. Additionally, socio-demographic factors, including age, gender, digital literacy, country, and trust in the provider, are used as control variables. The presented model is incomplete and will be tested in the quantitative study.

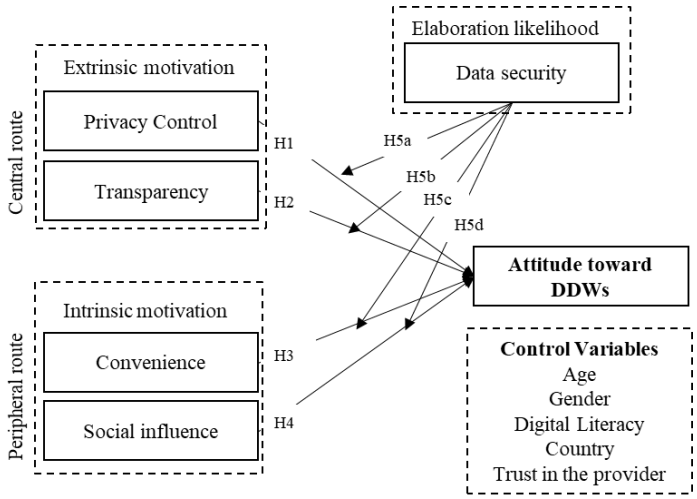

Figure 1. Research model.

Privacy control significantly increases the perceived benefit of using technology and perceived privacy in general (Cheng et al., 2021; Chang et al., 2018). DDWs are privacy-enhancing technologies that enable individuals to control their privacy. Hence, potential users expect to have complete control over their personal information inside DDWs and while sharing their information through DDWs. One participant in the qualitative study mentioned: "*I would need to be able to decide what information I give out and what not. And I would need to decide very easily what I want to give*." (Interviewee 3). If

DDWs promote complete privacy control for their users, the attitude toward the platforms will increase. Therefore, it is hypothesised:

H1: Privacy control will positively influence attitude.

Users who pay attention to transparency are more aware of information privacy (Xu, 2019). Individuals need to upload their information to the platform to use DDWs. Hence, potential users expect DDW platforms to transparently and clearly explain how their information is handled inside the platforms. In the qualitative study, participants expressed a clear desire for transparency. For instance, one participant mentioned: "*The more transparent the relationship between the manufacturer or developer of this platform and the person trying to use or want to use, the more willing the person is to use it.*" (Interviewee 18). If DDW providers guarantee transparent communication between users and platforms, the attitude toward the platforms will increase. Therefore, it is hypothesised:

H2: Transparency will positively influence attitude.

Inconvenience is one of the reasons for avoiding the adoption of privacy-enhancing technologies and practices (Zou et al., 2020; Coopamootoo, 2020). As a new technology, DDW platforms should build a user-friendly interface and provide more convenient service than current online information-sharing methods. One participant in the qualitative study mentioned: "*It would be super comfortable instead of having so many documents around, fast access to data all the time, and not having to look for the physical copies or the physical documents every time you need something.*" (Interviewee 10). If DDWs become a more convenient service in comparison to the current methods of information sharing, the attitude toward the platforms will increase. Therefore, it is hypothesised:

H3: Convenience will positively influence attitude.

Social influence plays a significant role in explaining technology adoption (Venkatesh et al., 2012). DDWs are new technologies. Hence, if family or friends use the platforms, this will help to form an attitude toward DDWs. One participant mentioned: "*If my friends or my parents or someone told me that it was very good, I would use it.*" (Interviewee 24). If important others believe that they should use DDWs, the attitude toward the platforms will increase. Therefore, it is hypothesised:

H4: Social influence will positively influence attitude.

Information security awareness increased privacy concerns and risks (Ortiz et al., 2018). Hence, potential users may pay more attention to security measures implemented in DDWs. It is argued that individuals with deep concerns regarding data security will focus on their ability to control their privacy and transparent communication between DDWs and their users. It is also argued that for individuals with low concerns regarding data security, convenience and recommendations from friends and family will play a more significant role in shaping attitudes toward DDWs. Therefore, it is hypothesised:

H5a (b): Data security will moderate privacy control (transparency) and attitude in such a way that the relationship will be stronger among users with high data security.

H5c (d): Data security will moderate convenience (social influence) and attitude in such a way that the relationship will be weaker among users with high data security.

6 Conclusion and next steps

This study identified extrinsic (privacy control, transparency) and intrinsic (convenience, social influence) motivations to form an attitude toward DDWs, adopting the motivation theory. The research model is built based on the elaboration likelihood model and qualitative study results. The proposed model will be improved and then tested with data from Austria, Romania, and Spain. The study contributes to privacy-enhancing technology adoption literature by identifying motivations for DDW adoption and enhancing the theoretical perspective on data security. As for the limitations, the study considers data security a unified concept without addressing the role of trust and contextual factors. Hence, future studies can examine the role of legal frameworks, cultural norms, other privacy-enhancing solutions, and ethics.

7 Acknowledgements

This work was supported by the European Union's Horizon 2020 program (SOTERIA project, Grant ID: 101018342), with Audencia Business School as a consortium partner. We also thank Fundação para a Ciência e a Tecnologia (FCT) for the program UIDB/04152/2020 – Centro de Investigação em Gestão de Informação – MagIC (NOVA IMS).

References

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). *The consumer-data opportunity and the privacy imperative*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Ashuri, T. (2024). Data management as a promise: The case of 'I.' *Computers in Human Behavior Reports*, *15*, 100462.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*, 1017–1041.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3–4), 245–270.

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: does control over personal information, user awareness and security notices matter? *Information Technology & People*, *28*(3), 426–441.

Bhattacherjee, A., & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *MIS Quarterly*, *30*, 805–825.

Bracamonte, V., Pape, S., & Loebner, S. (2022). "All apps do this": Comparing privacy concerns towards privacy tools and non-privacy tools for social media content. *Proceedings on Privacy Enhancing Technologies*, *3*, 57–78.

Brown, L. G., & McEnally, M. R. (1992). Convenience: Definition, structure, and application. *Journal of Marketing Management (10711988)*, *2*(2).

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly*, *35*(3), 445–459.

Cheng, X., Su, L., Luo, X., Benitez, J., & Cai, S. (2021). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *31*(3), 1–25.

Cichy, P., Salge, T. O., & Kohli, R. (2021). Privacy concerns and data sharing in the internet of things: Mixed methods evidence from connected cars. *MIS Quarterly*, *45*(4), 1863–1892.

Coopamootoo, K. P. L. (2020). Usage patterns of privacy-enhancing technologies. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 1371–1390.

Deci, E. L. (1976). Notes on the theory and metatheory of intrinsic motivation. *Organizational Behavior and Human Performance*, *15*(1), 130–145.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316.

European Commission. (2023). *European Digital Identity*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

European Union Agency for Cybersecurity. (2019). *ENISA's PETs Maturity Assessment Repositoryo Title*. https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository

Fischer-Hbner, S., & Berthold, S. (2017). Privacy-enhancing technologies. In *Computer and Information Security Handbook* (pp. 759–778). Elsevier.

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408–1416.

Harborth, D., & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *51*(1), 51–69.

Hu, X., Chen, Z., Davison, R. M., & Liu, Y. (2022). Charting consumers' continued social commerce intention. *Internet Research*, *32*(1), 120–149.

Kwak, D.-H., Ma, X., Polites, G., Srite, M., Hightower, R., & Haseman, W. (2018). Cross-level moderation of team cohesion in individuals' utilitarian and hedonic information processing: Evidence in the context of team-based gamified training. *Journal of the Association for Information Systems, Forthcoming*.

Lin, K.-Y., & Lu, H.-P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior*, *27*(3), 1152–1161.

Neves, C., Oliveira, T., & Karatzas, S. (2023). The impact of sustainable technologies in the perceived well-being: The role of intrinsic motivations. *International Journal of Human–Computer Interaction*, 1–12.

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, *61*, 404–414.

Ortiz, J., Chih, W.-H., & Tsai, F.-S. (2018). Information privacy, consumer alienation, and lurking behavior in social networking sites. *Computers in Human Behavior*, *80*, 143–157.

Petty, R. E., & Cacioppo, J. T. (1986). *The Elaboration Likelihood Model of Persuasion BT - Communication and Persuasion: Central and Peripheral Routes to Attitude Change* (R. E. Petty & J. T. Cacioppo, Eds.; pp. 1–24). Springer New York.

Petty, R. E., Cacioppo, J. T., & Goldman, R. (1981). Personal involvement as a determinant of argument-based persuasion. *Journal of Personality and Social Psychology*, *41*(5), 847.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Guest editorial: Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly*, *37*(4), iii–xviii.

Silva, P., Gonçalves, C., Antunes, N., Curado, M., & Walek, B. (2022). Privacy risk assessment and privacy-preserving data monitoring. *Expert Systems with Applications*, *200*, 116867.

SOTERIA. (2023). *SOTERIA, user-friendly secured personal data management platform*. https://www.soteria-h2020.eu/

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*.

Xu, Z. (2019). An empirical study of patients' privacy concerns for health informatics as a service. *Technological Forecasting and Social Change*, *143*, 297–306.

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., & Schaub, F. (2020). Examining the adoption and abandonment of security, privacy, and identity theft protection practices. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–15.