Online privacy literacy and users' information privacy empowerment: the case of GDPR in Europe

Christine Prince
ISG – Campus Paris Ouest, Paris, France
Nessrine Omrani
Paris School of Business, Paris, France, and
Francesco Schiavone
Università degli Studi di Napoli Parthenope, Napoli, Italy and Paris School of Business, Paris, France

Received 8 June 2023
Revised 3 October 2023
10 November 2023
Accepted 18 December 2023

Abstract

Purpose – Research on online user privacy shows that empirical evidence on how privacy literacy relates to users' information privacy empowerment is missing. To fill this gap, this paper investigated the respective influence of two primary dimensions of online privacy literacy – namely declarative and procedural knowledge – on online users' information privacy empowerment.

Design/methodology/approach – An empirical analysis is conducted using a dataset collected in Europe. This survey was conducted in 2019 among 27,524 representative respondents of the European population.

Findings – The main results show that users' procedural knowledge is positively linked to users' privacy empowerment. The relationship between users' declarative knowledge and users' privacy empowerment is partially supported. While greater awareness about firms and organizations practices in terms of data collections and further uses conditions was found to be significantly associated with increased users' privacy empowerment, unpredictably, results revealed that the awareness about the GDPR and user's privacy empowerment are negatively associated. The empirical findings reveal also that greater online privacy literacy is associated with heightened users' information privacy empowerment.

Originality/value – While few advanced studies made systematic efforts to measure changes occurred on websites since the GDPR enforcement, it remains unclear, however, how individuals perceive, understand and apply the GDPR rights/guarantees and their likelihood to strengthen users' information privacy control. Therefore, this paper contributes empirically to understanding how online users' privacy literacy shaped by both users' declarative and procedural knowledge is likely to affect users' information privacy empowerment. The study empirically investigates the effectiveness of the GDPR in raising users' information privacy empowerment from user-based perspective. Results stress the importance of greater transparency of data tracking and processing decisions made by online businesses and services to strengthen users' control over information privacy. Study findings also put emphasis on the crucial need for more educational efforts to raise users' awareness about the GDPR rights/guarantees related to data protection. Empirical findings also show that users who are more likely to adopt self-protective approaches to reinforce personal data privacy are more likely to perceive greater control over personal data. A broad implication of this finding for practitioners and

The authors want to thank the reviewers of this journal for their valuable and constructive comments and suggestions which helped to improve the manuscript. The authors also want to thank the cultural association "Knowmedtech" (Italy) for the support in the development and conceptualization of this article.

Information Technology & People
Vol. 37 No. 8, 2024
pp. 1-24
Emerald Publishing Limited
0959-3845
DOI 10.1108/ITP-05-2023-0467

E-businesses stresses the need for empowering users with adequate privacy protection tools to ensure more confidential transactions.

Keywords Information literacy, Survey, Information management, Privacy, Knowledge integration, End users

Paper type Research paper

Introduction

In today's digital environment, data-driven firms collect, store and process data about users at an escalating level, powered by emergent intrusive technologies such as AI, GPS, data mining software, IoT based devices and others (Emami-Naeini *et al.*, 2017; Kortesniemi *et al.*, 2019; Urban *et al.*, 2019; Kumar, 2023). This data-sharing environment is likely to reveal extensive personal information – tracked and shared by third party business partners – that could be used to identify a specific individual, buying patterns, financial and health records, etc. thus leading to privacy leakage among the involved parties in data flows (Conger *et al.*, 2012; Prince, 2018; Kortesniemi *et al.*, 2019; Kretschmer *et al.*, 2021; Maier *et al.*, 2023). For example, IoT and AI automated-based decision making have been widely deployed in support of tracking, collecting, and processing personal data of smartphone users and other devices to infer users' habits, behavior and for other commercial and marketing purposes, which emphasizes users' interest for control and protection of his own data.

Consequently, control over personal information is vital to address the threats of privacy invasive practices and ensure users' privacy (Gerlach *et al.*, 2018; Hagendorff, 2018; Kretschmer *et al.*, 2021).

Yet, web users have limited control over personal information management (Demmers *et al.*, 2018; Masur, 2020; Bornschein *et al.*, 2020; Prince, 2018; Ooijen and Vrabec, 2019; Sanchez-Rola *et al.*, 2019; Kretschmer *et al.*, 2021). For instance, a recent empirical study on 65 digital native users by Maier *et al.* (2023) revealed that many users reported feelings of powerlessness and lack of control in protecting their own data. This coincides with findings in other relevant literature (Hartman-Caverly and Chisholm, 2023; Hagendorff, 2018).

To ensure such control, the lately introduced European General Data protection regulation (GDPR) in 2018 is established to protect and empower UE citizen data privacy by regulating businesses handling and processing of personal data. This includes control rights in terms of access, storage, objecting receiving direct marketing, transmission and erasing of data, etc., while requiring an increased user responsibility in protecting their private information through an informed and express consent. In line with this, online privacy literacy (OPL) should be regarded as a vital factor in Internet users' assessment of potential risks of disclosing/sharing personal information (Masur *et al.*, 2023; Masur, 2020; Hagendorff, 2018; Correia and Compeau, 2017).

Yet, evidence from prior research work showed that online users have no/little knowledge about the data companies and digital technologies track, collect, and store about them (Gordon, 2018; Demmers *et al.*, 2018; Boerman *et al.*, 2018; Urban *et al.*, 2019; Moran, 2020; Luria, 2023; Hartman-Caverly and Chisholm, 2023; Kumar, 2023), nor the regulations and rights related to information privacy (Prince *et al.*, 2023; Robinson and Zhu, 2020; Soumelidou and Tsohou, 2021; Kardos, 2021; Maier *et al.*, 2023). Further, prior recent studies evidenced that – to date – no research has been found that surveyed the impact of GDPR on users' control over personal data flows with few exceptions (Ooijen and Vrabec, 2019; Bornschein *et al.*, 2020; Kretschmer *et al.*, 2021) though they stressed the need for such investigation.

Prior research highlights persisting privacy risks for online users since the GDPR went into effect. In a study that evaluates the influence of GDPR on Internet users in the context of web tracking, based on a manual analysis of 2000 popular websites across the world including EU located and non-EU hosted websites, results reveal that web tracking is still

prevalent even after the GDPR enactment. A vast majority of websites perform web tracking before providing any notice to users (Sanchez-Rola *et al.*, 2019). Likewise, based on a user study involving 470 participants on Amazon Mechanical Turk (Linden *et al.*, 2018), showed that though there was a positive change in the attractiveness and simplification of EU privacy policies since the GDPR enforcement, many privacy policies still do not comply with several key provisions on data protection set by the GDPR. This finding coincides with results revealed by Kretschmer *et al.* (2021). In their recent study that analyzes the literature that assesses the implications of GDPR legislation on personal data processing on the web, in particular, about how cookies consent notices, privacy policies and fingerprinting were impacted by the GDPR enactment, their study showed that most of these policies still lack information required by the GDPR. Most importantly, they also revealed the lack of user control by making it impossible to opt-out of non-essential data processing, accessing, or deleting. The non-functional cookies, often set by third-party websites, lead to important privacy leakage due to the prevalence of third-party trackers. Thus, given the complexity of technology used to manage data obtained from multiple websites, user privacy threats persist after the GDPR enactment. In the same vein, in a study that measures the Impact of the GDPR on data sharing in Ad Networks, findings revealed that the amount of tracking among online advertising companies was not affected since the GDPR enforcement though, highlighting its crucial impact on users' privacy (Urban *et al.*, 2020).

Thus, while these few advanced academic studies made systematic efforts to measure changes occurred on websites at the time the GDPR came into effect, it remains unclear, however, how individuals perceive, understand, and apply the GDPR rights/guarantees and their likelihood to strengthen users' information privacy control. Therefore, examining how privacy literacy affects users' information privacy empowerment has become a topic of common interest among scholars and practitioners (Ooijen and Vrabec, 2019; Bornschein *et al.*, 2020; Livingstone *et al.*, 2021). Yet, there is limited empirical evidence casting light on this relationship. In specific, our analysis of extant literature showed lack of research that incorporates both declarative and procedural knowledge dimensions of privacy literacy in a comprehensive model to examine their respective impact on perceived control over personal data privacy. Further, prior research on information privacy bears some limitations. Research work by Ooijen and Vrabec (2019) performed an analysis on the existing literature to understand how the GDPR principles can help maintain users' control over personal data. Although their study provides important steps for understanding the effects of GDPR on information privacy, empirical evidence about the effects of GDPR on users' privacy empowerment from users' perspective is notably lacking. Furthermore, based on a field study about the GDPR practices, Bornschein *et al.* (2020) investigates how the visibility and choice offered via website cookie notifications are likely to impact consumer privacy power and risk perceptions. Despite its substantial contributions to understanding the effects of cookie notice and choice on consumers' perceived power, they limited the scope of the analysis of GDPR provisions to the notice and choice.

Nonetheless, the GDRP aims beyond providing users with "notice" about their personal information collection and use practices and "choice" about how their personal data may be processed. This regulation is also intended to consider more substantive limitations on data processing and broader restrictions/requirements such as the right to object receiving direct marketing, the right to correct, the right to be forgotten/data deletion, data portability or even the right to refuse algorithmic/AI-based automated decision making. It has been shown that effective privacy protection should avoid adopting a mere "notice" and "choice" systems. Instead, considering European-style protections, such as the right to erase data and the right to be forgotten is recommended (Massara *et al.*, 2021). Accordingly, our study has a larger scope that considers those broader requirements. In particular, how users' knowledge and

applications of those rights are likely to strengthen users' privacy empowerment (perceived control over personal data).

The paper's main contribution to the current academic debate is that while the effectiveness of the GDPR on users' information privacy empowerment has been addressed from a purely academic point of view (Ooijen and Vrabec, 2019), to the best of our knowledge, there has not been much empirical analysis on the topic from user-based perspective. To fill this gap, the present paper aims to understand the levels of privacy awareness and skills (OPL) among EU citizens and their influence on information privacy empowerment, by combining legal insights from the GDPR privacy rights/provisions with privacy protective actions/strategies. Hence, it takes a user-based approach, focusing on users' awareness/knowledge and experiences with the GDPR privacy rights and skills related to data protection.

Our study contributes empirically to the emerging body of research on the role of privacy literacy on online users' information privacy perceived control, drawing upon a quantitative-based study by means of a large and representative sample of more than 27,000 respondents in 2019. The data aims to explore awareness of GDPR in particular, as well as more general opinions and behaviors relating to data sharing and data protection. An econometric model is performed to study the link between privacy perceived control and online privacy literacy. In a nutshell, the purpose of the current paper is to elaborate on the effects of the European GDPR and online users' privacy self-protection on their perceived control over personal data.

Based on a review of literature pertaining to online privacy (Xu *et al.*, 2012; Trepte *et al.*, 2015; Masur *et al.*, 2017, 2023; Weinberger *et al.*, 2017; Boerman *et al.*, 2018; Masur, 2020; Bornschein *et al.*, 2020, Livingstone *et al.*, 2021; Kumar, 2023; Hartman-Caverly and Chisholm, 2023), we make the following three contributions:

First, examine how individuals' awareness and knowledge about privacy protective regulations and rights are likely to impact their perceived control over personal data flows. In particular, how effective is the General Data protection regulation (GDPR) in strengthening individuals' perceived control over personal data flows. Second, how much privacy protective actions/measures are likely to affect their perceived control over personal data flows. Third, how privacy literacy influences web users' perceived control over personal data flows. Thus, on a theoretical level, this study deepens our understanding of how the GDPR may influence users' privacy empowerment and offers an empirical link between the domains of user's privacy literacy and user privacy empowerment. Further, the current paper investigates jointly the effects of declarative and procedural knowledge on users' information privacy empowerment that warranted further exploration.

The remainder of the paper is structured as follows: Section 2 presents a review of relevant research work and outline the theoretical framework of our research paper; section 3 introduces data and research methodology; section 4 provides a summary of data analysis results and section 5 concludes with a discussion of research findings and presents theoretical and practical implication and direction for future research perspective.

Related work

Online privacy literacy (OPL)

In the era of big data, advanced digital technologies, and the growing use of AI-automated decision making, privacy literacy has become fundamentally important, but people have little awareness about the GDPR data protection rights/guarantees, online tracking practices and skills related to data protection (Maier *et al.*, 2023; Kardos, 2021; Desimpelaere *et al.*, 2020; Urban *et al.*, 2019). Privacy literacy has been recognized as an important factor in online data protection behavior (Sindermann *et al.*, 2021). Hartman-Caverly and Chisholm (2023) emphasized the important role of privacy literacy in empowering one's self-awareness of his/

her own privacy to regulate information privacy online. Reviewing prior studies on online user privacy, however, has revealed that research in this area is at early stages (Ooijen and Vrabec, 2019; Bornschein *et al.*, 2020; Pingo and Narayan, 2017; Livingstone *et al.*, 2021; Masur *et al.*, 2023; Kumar, 2023).

In an attempt to address the problem related to children privacy literacy online, a recent work by Livingstone *et al.* (2021) emphasized the important role of educating them better understanding, managing and preserving their privacy in an increasingly complex and "datafied" digital economy. Thus, they argue that it is not sufficient to gain functional skills/coping strategies to manage their privacy setting but also need a deep knowledge and understanding of digital environments data tracking practices to develop a sense of empowerment. Further, their study contends that online environments are powered not only by "shared" data but also by implicit pervasive "inferred/profiling" data and "data tracking" technologies. Therefore, this underpins the crucial role of privacy literacy in managing users' privacy.

Furthermore, in an empirical study based on interviews combined with ethnography with university students, Pingo and Narayan (2017) examine participants' perceptions, awareness, and use of social media. Their study sparks the need to incorporate privacy literacy as a key dimension of information literacy.

Drawing on prior research on online privacy literacy (Trepte *et al.*, 2015; Masur, 2020; Bartsch and Dienlin, 2016; Park and Jang, 2014; Wissinger, 2017; Masur *et al.*, 2023; Kumar, 2023) and combining with other research work pertaining to online privacy literature (Debatin *et al.*, 2009; Xu *et al.*, 2012; Arachchilage and Love, 2014; Correia and Compeau, 2017; Masur, 2020; Prince *et al.*, 2023), we define online privacy literacy (OPL) as Internet users' knowledge (awareness) and skills (behavior) related to information privacy protection.

While "knowledge" refers to users' awareness of websites and firms' practices in terms of personal data collection, knowledge about technical aspects of online privacy and data protection, and knowledge about privacy protective regulation and rights," skills" in its turn, designates users' privacy protective actions and measures. It is worth noting that while the former is referred to as "declarative knowledge", the latter is named "procedural knowledge".

In a study that investigates Facebook users' privacy awareness and online privacy attitudes and behaviors, Debatin *et al.* (2009) asserted that the concept of OPL involves: (1) an informed concern for one's privacy – in that, users must be well-informed about the potential negative implications of SNS on their privacy – and (2) effective strategies to protect it. Therefore, it is essential to acknowledge that both knowledge and skills are necessary to mitigate the negative consequences related with personal data sharing. Consistent with this evidence, Correia and Compeau (2017) also stressed the importance of privacy awareness (knowledge). They argue that users' privacy protective actions depend heavily on their awareness of the potential threats/consequences of sharing private information so he may be able to restrict their sharing correspondingly. Further, their study stated that awareness requires that user's "education" about regulations, companies practice in terms of personal data collection and understanding of technologies collecting and processing this data. In accordance with this assumption, Masur (2020) claimed that user awareness is key requisite in developing a sense of literacy and without the awareness of privacy intrusive practices/threats in the digital environment, procedural knowledge becomes useless. The author contends that online privacy literacy should provide users with knowledge and skills to protect their privacy against invasive practices by external influences, including authoritarian governments. In a nutshell, the author stressed the importance of both knowledge and skills as underlying dimensions of OPL to enable individuals to have control over their personal information. Thus, Masur (2020) argues that privacy literacy incites user to become an "agent".

Nonetheless, in a world of ubiquitous surveillance and wide-scale data collection, privacy intrusions and erosions are often invisible and difficult to control (Tavani and Moor, 2001; Demmers *et al.*, 2018). For instance, machine and algorithmic automated decision making exacerbates and reduces greatly individual ability to claim control and agency. In this realm, Hagendorff (2018) confirmed that online privacy literacy contributes to empowering technology users to control personal data. He asserted that privacy literacy goes beyond merely changing privacy settings. Privacy literacy should also encompass users' awareness of back-end invisible data collections and awareness of the privacy loss by default setting. His work also revealed that technology users know little about user tracking practices (about explicit and implicit data practices). This coincides with findings made by a recent study by Desimpelaere *et al.*, 2020). Based on in-depth interviews research design with 10 parents and 9 children, their study showed, that in the era of digital age, children lacked knowledge about both explicit and invisible online tracking practices. Their findings suggest that privacy literacy contributes substantially to enhancing users' understanding of companies' data practices and empowering them to protect personal data privacy. This is also reported by a recent work by Hartman-Caverly and Chisholm (2023) which suggests that robust privacy literacy instruction should uncover the backend implicit processes of personal data collection and manipulation.

Furthermore, in a study that investigates the effects of conceptual knowledge and procedural knowledge on users' self-efficacy in relation to phishing attacks, Arachchilage and Love (2014) put emphasis on user security "education" as technology alone can't address alone critical IT security issues. Their research focuses on the "human" aspect of performing security using a given protective measure. This measure does not necessarily have to be an IT anti-phishing tools; rather it could be behavior such as anti-phishing "education".

Survey-based research by Weinberger *et al.* (2017) that examines determining factors of OPL in a sample of 160 Israeli students, shows that users' information privacy concerns and users' self-efficacy as the most influential factors in understanding OPL. Their study claimed that OPL involves both "declarative" and "procedural" knowledge. However, their study falls short of its claims. It didn't account for online users' knowledge about privacy protective regulations and rights.

Bornschein *et al.* (2020) examined the effects of notice visibility and choice in websites' information collection practices on consumers' privacy power. Despite its significant contributions to understanding how visibility and choice offered via website cookie notifications are likely to impact consumer perceived power over personal information, privacy literacy, was solely concerned with "front-end" features where users have the "consent" and "choice". However, this is likely to lead to overlook many of back-end implicit practices of personal data tracking and processing such as the automated decision making and inferred profiling (Hartman-Caverly and Chisholm, 2023; Kumar, 2023). The GDPR regulation is also intended to consider more substantive limitations on data processing and broader restrictions/requirements such as the right to refuse algorithmic-based automated decision making that we consider examining in our study.

In more recent research, Prince *et al.* (2023) conceptualized Internet users privacy concerns through declarative knowledge (awareness) and procedural knowledge (application). While this research provides several important insights, particularly in understanding how users' privacy literacy is likely to mitigate their concerns over personal data, their study bears some methodological issues in terms of OPL measurement. Their study lacks the measurement of declarative knowledge relating to firms' practices in terms of data collection, processing and storage. Further, as their study was based on data collected prior to the GDPR enforcement, they didn't account for how the stricter GDPR provisions introduced in 2018 may help addressing online users' privacy concerns.

Consistent with the preceding discussion, this paper suggests that online privacy literacy is formed by both cognition (awareness) and application (Behavior) needed to protect one's personal information: While awareness designates the amount of knowledge, the application refers to the amount of behavior (Dinev and Hart, 2006; Correia and Compeau, 2017; Pingo and Narayan, 2017; Wissinger, 2017). In summary, it implies users' knowledge about platforms data collection and uses practices, data protection regulations, and knowledge about techniques and strategies they can apply to protect their privacy (Masur *et al.*, 2023).

User privacy empowerment

User privacy empowerment finds its origins in consumer empowerment and psychology literature (Van Dyke *et al.*, 2007; Alshibly and Chiong, 2015; Hagendorff, 2018; Prince, 2018; Bornschein *et al.*, 2020). This concept emphasizes the role of control over privacy. According to this premise, empowerment is related to control and is regarded as individual desire to control his environment.

The GDPR is established to enable users to exercise their control rights. In other terms, it is intended to provide data subjects with a "notice" (prior notification) about information collection and use practices. It stressed therefore the need for transparency regarding personal data collection and use. As well, it emphasizes the need for a clear informed indication of agreeing personal data processing (Regulation (EU) 2016/679). Accordingly, it seeks to give him the "choice" (consent seeking): individuals should be granted an option to express consent about data collection and processing (Ooijen and Vrabec, 2019; Bornschein *et al.*, 2020). Similarly, Masur (2020) argued that data subject should have the right and the ability to decide for themselves when and to which extent information about himself should be collected, processed or disseminated/shared with others. This has been referred by the author as "self-determination". Hence, this concept acknowledges and emphasizes users' privacy self-agency. Likewise, Pingo and Narayan (2017), Hagendorff (2018) advanced that there is shift of responsibility from government towards users to exert control over their online privacy.

According to Tavani and Moor (2001), the concept of empowerment goes beyond restricting "access" to one's personal information. Individual should be able to control the dissemination of personal data. They stressed the role of control in privacy management, which is embodied by three major dimensions: consent, choice and correction.

Extending on prior research on individual's empowerment in research that investigates the effects of consumer privacy empowerment on privacy concerns in E-commerce, Van Dyke *et al.* (2007), provided a comprehensive understanding of user's privacy empowerment. Their study showed that users privacy concerns are related to their perceived control over personal data. The authors highlighted the underlying dimensions of such control: the "Notice", the "Choice" and the "Access". Following this rationale, individuals should have prior "notification" about personal data collection, use and sharing among the involved parties. The "choice" component designates the right to have an option of consent about data collection and use. The "access" refers to user ability to rectify, correct personal information about oneself, thereby allowing for a greater control against intrusive privacy practices.

Building on this, we suggest that the concept of user privacy empowerment embodies notions of "notice", "choice" (consent) and "access". It refers to individual perception of the extent to which he can control personal data dissemination and use. We apply this concept to refer to users' perceived control over personal data flows (Van Dyke *et al.*, 2007; Midha, 2012; Bornschein *et al.*, 2020).

Online privacy literacy and users' privacy empowerment

The GDPR principals suggest that data subject should be "notified" about firm's practices in terms of data collection (awareness). As previously mentioned, it also established a set of other guarantees/rights to ensure information privacy control. How the awareness about GDPR rights/provisions is likely to influence his perceived control over personal data?

Declarative knowledge is likely to influence users' perceived control over personal information. A range of relevant studies on user privacy empowerment suggest that users feel more powerful if they are aware or receive notice about firms and websites practices in terms of personal data collection, use and sharing (Dinev and Hart, 2006; Prince, 2018; Bornschein *et al.*, 2020). This is also in line with research by Ooijen and Vrabec (2019) that argued that control requires knowledge/awareness about the consequences of negative risks associated with data sharing. Further, their study contended that control over personal information is tightly correlated with an express consent where individual may approve or object personal data gathering and processing. The same study stressed the informational complexity and individual's limited cognitive abilities in reading privacy-related information that require specific expertise "literacy" in terms of understanding. In addition, their research argued that informing data subjects about the existence of automated decision-making may result in fostering the informational perceived control over personal data processing. This echoes also some findings revealed by other relevant research work (Hagendorff, 2018; Livingstone *et al.*, 2021; Hartman-Caverly and Chisholm, 2023; Luria, 2023; Kumar, 2023). In a study the focuses on recommendation algorithms transparency (Luria, 2023), the author argues that users' often lack knowledge about how those algorithms work and what information they use, stressing therefore the important role of users' awareness in this regard to empower users with control over their information privacy. Further, Kumar (2023), argued that digital technologies such as sensors, IOT devices, algorithms are fueled by data derived from people and often used for prediction purposes. Still, users have little knowledge of what data is tracked and used by such technologies, emphasizing the impact of knowledge/awareness about digital data flows in enhancing users' control over information privacy.

The GDPR is believed to embody a state of user's empowerment in gaining greater control over their personal data (greater users' privacy empowerment) (Ooijen and Vrabec, 2019). A study by Kardos (2021) explores privacy literacy and personal data protection of law students. For this purpose, they conducted an online survey with 205 faculty law students in Hungary combined with in-depth interviews with 16 students. Their findings highlight the lack of knowledge among the surveyed students in relation to the identification of personal data. Moreover, results show that most study participants stated that they were unaware of GDPR data protection guarantees. Their findings suggest that privacy literacy should be improved to ensure higher levels of data protection. Likewise, Youn (2009) argued that users who are more knowledgeable about legislations and privacy rights tend to have a greater control over their personal data flows. Building on the above, we put the following hypothesis:

H1. Declarative knowledge is positively associated with user' privacy empowerment.

Regarding the link between procedural knowledge (skills and actions) and perceived control over personal data, and more specifically reading privacy policy statements and using cookie management tools, we believe that individuals with higher procedural knowledge may perceive themselves as having greater control over their personal information (Park and Jang, 2014). Their research stressed the importance of individuals' management of their personal information tracking and claimed that users who don't know how to effectively manage their information tracking are more likely to undergo conspicuous privacy intrusions. In the same vein, in a survey about young adults' online privacy practices during job search, Hargittai and Litt (2013) showed that privacy skills (the "know how") relate to people likelihood to

manage their privacy. Similarly, Boerman *et al.* (2018) claimed that privacy management is particularly important as legislation falls short in providing privacy protection. Li *et al.* (2011) asserted that the extent to which individuals are informed about website privacy policy statement assists in reassuring and empowering users for privacy preservation. This underpins the importance of procedural knowledge in ensuring users' control over personal data privacy. It is worth noting that Xu *et al.* (2012) distinguish between technological and non-technological privacy self-protection mechanisms. While the former comprises privacy-enhancing technologies that allow control over personal data flows including anonymous web browsing, cookie management tools (privacy setting change), privacy enhancing features that enables limit personal data access, use, disclosure, etc.), the latter includes approaches such as reading privacy policy, complaining to third party organization or directly to the online company. Within the scope of our paper, we focus on investigating both approaches, specifically reading and understanding privacy policy and customizing cookie tracking and privacy policy banner by changing privacy settings. Hence, we hypothesize the following:

H2. Procedural knowledge is positively associated with user' privacy empowerment.

In a survey-based study on 630 Facebook users by Bartsch and Dienlin (2016), findings revealed that users reporting higher online privacy literacy safety are believed to express higher perceived privacy safety. It is worth noting that perceived privacy safety embodied a state of control over physical, psychological or material harm. In support of this assumption, we believe that users expressing higher privacy literacy perceived greater control over personal data. Consistent with this result, in a study that investigates mobile-based privacy literacy among young adults, Park and Jang (2014) emphasized the important role of privacy literacy – that is shaped by both knowledge and skills – in empowering users with sense of control over information privacy. Arachchilage and Love (2014) asserted that "procedural knowledge" is significantly close to the idea of "know how" and the declarative knowledge is "now that". Furthermore, he explained that such declarative knowledge allows us to explain why, hence the distinction of "know how" and "know why". In accordance with this premise, Prince *et al.* (2023) argued that the two dimensions of declarative and procedural knowledge are likely related by seldom associated, with their relationship being underexplored. Following this rationale, we propose that both procedural and declarative knowledge positively impact perceived control over personal data. Likewise, in an experimental study that examines users' information privacy concerns in the context of location-based services that draws upon control agency theory, Xu *et al.* (2012) claimed that there are two approaches to strengthen users' perceived control over personal data: (1) Self-agency via self-protection (self-protection approach) and (2) others proxy agency (proxy control). Self-agency designates personal control enhancing mechanisms. Accordingly, an individual acts as a control agent in protecting his/her information privacy, whereas other agencies refer to others that act as a control agent to protect individuals' privacy (such as governmental regulations). Their findings revealed that both agencies are likely to impact their privacy concerns. They argue that self-protective approach leads to feel greater autonomy and provides users with control over his personal data flows and therefore with a sense of self-agency, reducing the effects of proxy control via governmental regulations. On the other hand, it is postulated that government regulations set privacy protection rights that allow users to believe that companies will protect their disclosed data, conceding therefore personal control and allowing the regulations to protect their personal data on their behalf. The rationale behind this premise is that individuals tend to minimize the amount of cognitive effort pertaining to information processing and do not process information more than necessary. Hence, if one of the two agencies is sufficient to make risk-free judgments, the existence of other mechanisms may not matter. A widely agreed upon argument is that users with higher privacy literacy

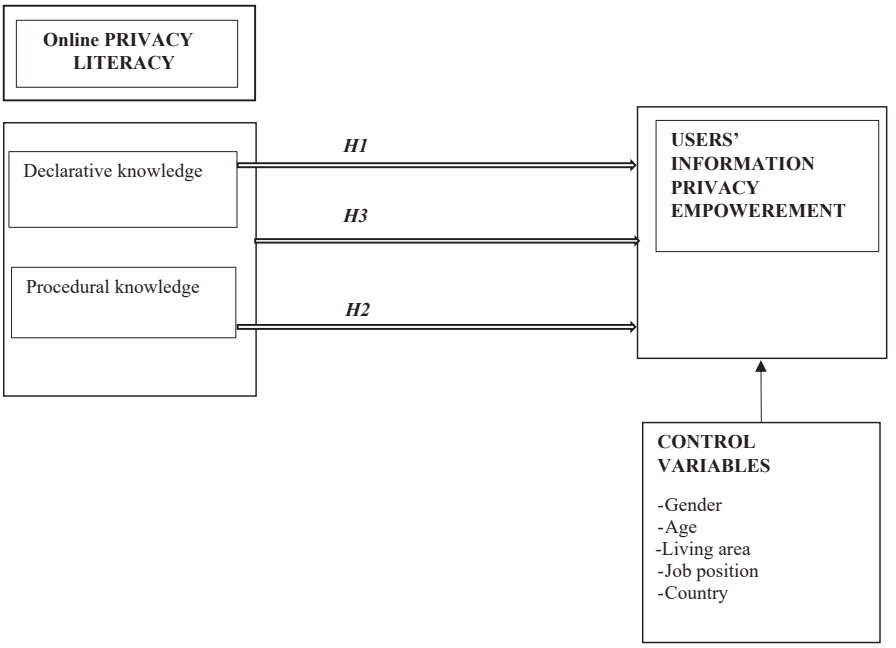
who have the knowledge and skills are more likely to perceive heightened information privacy control (Masur, 2020; Hagendorff, 2018; Prince *et al.*, 2023). In line with this, Livingstone *et al.* (2021) study emphasized that online privacy literacy involves both users' knowledge and agency regarding their personal data flows online. In accordance with those premises, we examine the joint effect of declarative and procedural knowledge and its likely impact on users' perceived control. Hence, we assess the effect of declarative knowledge (Internet users' knowledge about privacy GDPR provisions and rights, knowledge about firms and websites practices in terms of personal data collection, knowledge about existence of public authority to report complaint of privacy violation) and the procedural knowledge (self-protective actions and strategies used by Internet users: In the scope of this paper, reading privacy policy statement and changing privacy settings) on users' privacy empowerment. Thus, we argue that online users' who report higher level of OPL also perceive increased control over information privacy. Thus, the above discussion leads us to hypothesize the following:

H3. Online privacy literacy is positively associated with users' privacy empowerment.

Therefore, Figure 1 presents a conceptual model that illustrates the studied variables and their hypothesized interrelations in understanding users' information privacy empowerment. The research model describes that users' privacy empowerment is determined by both "self-agency" procedural knowledge) and "others agency" (declarative knowledge) approaches.

Data and research methodology

The dataset used in this paper is collected in Europe, namely the Eurobarometer 487. This survey was conducted in 2019 among 27,524 representative respondents of the European population. It was commissioned by the European Commission Directorate-General for



Source(s): Authors' own work

Figure 1.
Conceptual framework of online users' information privacy empowerment and online privacy literacy

Justice and Consumers to explore users' awareness about the GDPR in particular, as well as more general opinions and behaviors relating to data sharing and data protection. In the Eurobarometer 487, we focused on Internet users. After data cleaning, we obtained a dataset of more than 15,000 observations that covered 29 EU countries.

Variables and measurement

Variables. The endogenous variable is the level of consumer empowerment. Respondents were asked about the level of control they have over the information provided online (e.g. the ability to correct, change or delete this information).

The variable takes the value 2 if the individual feels having a complete control over the information provided, 1 if he feels some control or depending on the website or application, and 0 if he feels no control at all.

The variable of interest is OPL. The two dimensions of OPL, namely "declarative knowledge" and "procedural knowledge" were derived from prior privacy studies (Masur *et al.*, 2017; Trepte *et al.*, 2015; Weinberger *et al.*, 2017).

Other variables used as control variables were also linked to consumer empowerment, such as demographics (gender, age), job position, paying bills as a proxy for wages, living area and country.

Descriptive statistics

This study adopted items that estimate web user's knowledge about laws and regulations related to personal data protection and items that assess the self-protective actions adopted to protect privacy. Procedural privacy knowledge was measured using two items that referred to the actions taken by the individual that enabled him to enforce security and privacy in handling information privacy through (1) changing the privacy settings of the personal profile from the default settings (e.g. to delete browsing history or delete cookies) and (2) reading privacy statement.

Declarative knowledge was measured using items related to the awareness of users about (1) companies and organizations practices in terms of data collection and further uses conditions; (2) the GDPR; (3) the existence of a public authority to report complaint against privacy violations, and (4) the rights to: access the data, object to receiving direct marketing, correct data if it is wrong, to delete data and to be forgotten, have a say when decisions are automated, move data from one provider to another.

Other variables used as control variables were also linked to consumer empowerment, such as demographics, job position, living area, and wage.

The age of the individuals ranged from 15 to 98. The gender variable takes the value 1 if male and 0 if female. Job position is measured using the following variables: unemployed, self-employed and employed. A set of mutually exclusive binary variables are used for "living area", which indicate whether the individual lives in a large town, a mid-sized town, or a rural area. "Paying bills" is used as a proxy to measure the wage indicating in what extend the individual has difficulties in paying bills at the end of the month.

Table 1 gives the descriptive statistics.

Data analysis

Ordered logit regression analysis is one of the most used approaches for modelling consumer behavior (Guadagni and Little, 1983). This method is commonly employed for ordered outcomes in social sciences (Borooah, 2002). Therefore, we apply ordered logit regression as our outcome variable reflect an underlying ordering. Hence, we estimate the following model:

Type of var	Description	Mean	Std dev	Min	Max
Endogenous variable					
User information privacy empowerment		0.873	0.661	0	2
Exogenous variables					
Control variables					
Gender	Female/male	0.453	0.497	0	1
Age (years old)	15–24	0.082	0.274	0	1
	25–39	0.198	0.398	0	1
	40–54	0.244	0.429	0	1
	55+	0.475	0.499	0	1
Age (years old)		51.908	18.141	15	98
Job position	Self-employed	0.069	0.253	0	1
	Employed	0.442	0.496	0	1
	Unemployed	0.488	0.499	0	1
Living area	Rural	0.337	0.472	0	1
	Middle town	0.375	0.484	0	1
	Large town	0.287	0.452	0	1
Paying bills	Having difficulties in paying bills at the end of the month (0: most of the time; 1: occasionally; 2: almost never)	1.594	0.640	0	2
Procedural knowledge					
Privacy settings	To change the privacy settings of the personal profile from the default settings on an online social network	0.542	0.498	0	1
Reading privacy statement	Reading privacy statements (0: do not read them at all; 1: read them partially; 2: read them fully)	0.820	0.691	0	2
Declarative knowledge					
Awareness – data collection conditions	Being informed about companies and organizations practices in terms of the conditions of the collection and further uses of the data provided (0: never, 1: rarely, 2: sometimes; 3: always)	1.622	1.069	0	3
Awareness – authority	Aware of the existing of a public authority responsible for protecting consumer rights regarding personal data (0: no; 1: yes, but don't know which public authority is responsible; 2: yes, and know which public authority is responsible)	0.815	0.748	0	2
Awareness – GDPR	Aware about the general data protection regulation (GDPR) (0: no; 1: yes, but don't know exactly what it is; 2: yes, and know what it is)	1.058	0.813	0	2
Awareness – rights–access data	Aware about the right to access the data (0: no; 1: yes, but have not exercised it; 2: yes, and have exercise it)	0.858	0.701	0	2
Awareness – rights–marketing	Aware about the right to object to receiving direct marketing (0: no; 1: yes, but have not exercised it; 2: yes, and have exercise it)	0.834	0.766	0	2
Awareness – rights–correct data	Aware about the right to correct data if it is wrong (0: no; 1: yes, but have not exercised it; 2: yes, and have exercise it)	0.795	0.698	0	2

Table 1.
Descriptive statistics

(*continued*)

Type of var	Description	Mean	Std dev	Min	Max
Awareness – rights–data deleted	Aware about the right to have data deleted and to be forgotten (0: no; 1: yes, but have not exercised it; 2: yes, and have exercise it)	0.722	0.680	0	2
Awareness – rights–a say	Aware about the right to have a say when decisions are automated (0: no; 1: yes, but have not exercised it; 2: yes, and have exercise it)	0.505	0.639	0	2
Awareness – rights–move data	Aware about the right to move data from one provider to another (0: no; 1: yes, but have not exercised it; 2: yes, and have exercise it)	0.649	0.696	0	2

Source(s): Authors' own work

Table 1.

$$\Pr(\text{Privacy Empowerment}i) = \beta\,\text{Demographics}i + \beta\,\text{Procedural knowledge} + \beta\,\text{Declarative knowledge} + \alpha i + \varepsilon i$$

Building on the literature review in the preceding section, user's privacy empowerment may be influenced by privacy knowledge and declarative knowledge and their joint effects.

Results

The results of the logistic regression estimation are reported in Table 2. Because we rely on cross-section data, we cannot account for endogeneity among the variables and the links between variables are correlational. To ensure the robustness of our results, we performed four model specifications, showing the results in blocks.

The first model gives results using only the items related procedural knowledge as exogenous variables. The second model adds declarative knowledge variables. In the third model, we introduce the demographics. In the fourth model, the "country" is incorporated. To account for the methodological issues related to multicollinearity effects between the "awareness about the GDPR" and the "awareness about the rights guaranteed by the GDPR", we performed a fifth model estimation. Hence, "awareness about the GDPR" is introduced without the "awareness about the different rights guaranteed by the GDPR". Empirical findings from these models show substantial robustness across the performed model specifications.

The results show, with respect to the variable of interest, procedural knowledge, a positive and significant (at 1%) link between procedural knowledge and user's privacy empowerment when looking at all the models. This means that there is a positive link between the level of perceived control users have over the information provided online on the one hand and changing the privacy settings from the default settings and reading privacy statements on the other hand. When looking at declarative knowledge, the link remains positive and significant at 1% for the items related to: data collection conditions, authority, the rights of data access, the right of a say. Thus, being informed about companies and organizations practices in terms of the conditions of data collection and further uses, being aware of the existing of a public authority responsible for protecting consumer rights regarding personal data, being aware about the right to access the data, being aware about the right to have a say when decisions are automated are found to have a positive link with users' level of perceived control over personal data. This link is negative and significant at 5% when looking at the awareness about the right to object to receiving direct marketing.

Table 2.
Online user information privacy empowerment – ordered logistic regression results

	(1)		(2)		(3)		(4)		(5)	
Online user information privacy empowerment										
Procedural privacy knowledge										
Privacy settings	0.621***	(0.034)			0.213***	(0.040)	0.235***	(0.041)	0.267***	(0.039)
Reading privacy statement	0.648***	(0.028)			0.696***	(0.031)	0.664***	(0.032)	0.696***	(0.031)
Declarative privacy knowledge										
Awareness – data collection and further uses conditions			0.449***	(0.020)	0.407***	(0.024)	0.417***	(0.024)	0.408***	(0.023)
Awareness – Authority			0.111***	(0.026)	0.139***	(0.030)	0.123***	(0.030)	0.146***	(0.029)
Awareness – GDPR			−0.058**	(0.025)	−0.023	(0.029)	−0.013	(0.030)	0.034	(0.028)
Awareness – rights–access data			0.136***	(0.033)	0.108***	(0.037)	0.106***	(0.038)		
Awareness – rights–marketing			−0.101***	(0.026)	−0.085***	(0.030)	−0.065**	(0.031)		
Awareness – rights–correct data			0.110***	(0.033)	0.043	(0.037)	0.048	(0.037)		
Awareness – rights–data deleted			0.051	(0.033)	0.046	(0.037)	0.036	(0.037)		
Awareness – rights–a say			0.182***	(0.030)	0.181***	(0.034)	0.160***	(0.035)		
Awareness – rights–move data			0.036	(0.029)	0.014	(0.033)	0.010	(0.034)		
Control variables										
Gender					0.001	(0.036)	0.012	(0.037)	0.021	(0.035)
Age										
15–24					*Ref*		*Ref*		*Ref*	
25–39					−0.223***	(0.062)	−0.221***	(0.062)	−0.224***	(0.060)
40–54					−0.332***	(0.064)	−0.319***	(0.064)	−0.346***	(0.061)
55+					−0.528***	(0.063)	−0.477***	(0.064)	−0.505***	(0.062)
Paying bills					−0.017	(0.030)	0.056	(0.034)	0.054*	(0.033)
Job position										
Unemployed					*Ref*		*Ref*		*Ref*	
Self-employed					0.025	(0.046)	0.032	(0.047)	0.011	(0.042)
Employed					−0.051	(0.043)	−0.023	(0.044)	−0.023	(0.068)

(*continued*)

Table 2.

	(1)	(2)	(3)		(4)		(5)	
Living area								
Rural area			*Ref*		*Ref*			
Middle-size town			0.024	(0.070)	−0.038	(0.071)	−0.012	(0.043)
Large-size town			0.026	(0.044)	−0.004	(0.044)	0.024	(0.046)
Country								
France					*Ref*		*Ref*	
Belgium					0.205	(0.130)	0.227*	(0.125)
The Netherlands					−0.186	(0.131)	−0.184	(0.126)
Germany					−0.453***	(0.140)	−0.475***	(0.134)
Italy					0.263**	(0.130)	0.266**	(0.125)
Luxembourg					0.324*	(0.185)	0.186	(0.174)
Denmark					0.099	(0.136)	0.087	(0.131)
Ireland					0.401***	(0.136)	0.411***	(0.130)
The UK					0.091	(0.137)	0.096	(0.130)
Greece					0.515***	(0.142)	0.431***	(0.136)
Spain					−0.142	(0.146)	−0.233*	(0.141)
Portugal					0.778***	(0.141)	0.755***	(0.137)
Finland					0.369***	(0.133)	0.343***	(0.127)
Sweden					0.009	(0.136)	−0.069	(0.131)
Austria					0.329**	(0.131)	0.341***	(0.125)
Cyprus					0.746***	(0.180)	0.700***	(0.173)
Czech Republic					0.270**	(0.135)	0.207	(0.129)
Estonia					0.300**	(0.146)	0.323**	(0.139)
Hungary					0.742***	(0.150)	0.723***	(0.143)
Latvia					−0.176	(0.144)	−0.193	(0.137)
Lithuania					0.377**	(0.150)	0.368***	(0.142)
Malta					0.873***	(0.193)	0.877***	(0.187)
Poland					0.877***	(0.145)	0.852***	(0.138)
Slovakia					0.391***	(0.139)	0.363***	(0.133)
Slovenia					0.248*	(0.150)	0.191	(0.144)
Bulgaria					0.017	(0.149)	−0.066	(0.142)

(*continued*)

Table 2.

	(1)		(2)		(3)		(4)		(5)	
Romania							−0.093	(0.140)	−0.073	(0.135)
Croatia							0.645***	(0.135)	0.633***	(0.130)
cut1										
_cons	−0.728***	(0.027)	0.656***	(0.047)	0.278***	(0.088)	0.620***	(0.135)	0.489***	(0.128)
cut2										
_cons	1.960***	(0.033)	3.551***	(0.058)	3.265***	(0.095)	3.665***	(0.141)		
cut3										
_cons	−1.182***	(0.020)	−1.023***	(0.047)	−1.174***	(0.111)	−1.394***	(0.155)	3.502***	(0.133)
N	13,930		15,689		15,483		15,483		13,435	

Note(s): Standard errors in parentheses, *$p < 0.10$, **$p < 0.05$, ***$p < 0.01$
Source(s): Authors' own work

The sociodemographic results, with respect to Age, taking people aged between 15 and 24 as the reference category, the link is negative, meaning that older people feel having less empowerment about their privacy. Regarding the Job Position, this link is not significant. In addition, living in a large town, a mid-sized town, or a rural area has no significant link with individuals' empowerment.

We also controlled the Country. The results of the three models show that, compared to the reference country – France – individuals living in Italy, Luxembourg, Ireland, Greece, Portugal, Finland, Austria, Cyprus, Czech Republic, Estonia, Hungary, Lithuania, Malta, Poland, Slovakia, Slovenia, and Croatia have more privacy empowerment, whereas individuals living in Germany expressed less privacy empowerment.

Discussion

In what follows, we discuss our empirical findings in relation to prior research work to better elucidate the key contributions of this paper to the privacy literature.

First, the ordered logit regression estimation revealed that the positive link between users' procedural knowledge and users' privacy empowerment is supported (H1). Particularly, results suggest that reading privacy policy statements and changing privacy settings of personal profile from the default settings (e.g. deleting browsing history or deleting cookies) are positively associated with heightened information privacy empowerment. In summary, empirical findings show that users who are more likely to adopt self-protective approaches to reinforce personal data privacy are more likely to perceive greater control over personal data. This result is consistent with the work by Xu *et al.* (2012) that highlighted that both technological and non-technological privacy self-protection approaches may lead to higher perceived control over personal data flows. This result corroborates also premises made by other relevant work that suggest that privacy self-management skills are particularly important as legislations fall short in providing privacy protection (Hargittai and Litt, 2013; Li *et al.*, 2011; Boerman *et al.*, 2018). This supports the results of recent research by Livingstone *et al.* (2021) that underlines that some functional skills such as changing privacy setting, reading privacy policies and navigating through conditions, etc., are necessary to empower children over their privacy.

Second, empirical findings also lend a partial support to the relationship between users' declarative knowledge and users' privacy empowerment (H2). For example, users' information privacy empowerment is found to be positively associated with the following: "awareness about data collection and further uses conditions", "awareness about the existence of a public authority to report complaint", "awareness about the right to access data", "awareness about the right to have a say when decisions are automated", and the "awareness about the right to correct data". Conversely, users' privacy empowerment is found to be negatively associated with the following: the "awareness about the GDPR" and the "awareness about the right to object receiving direct marketing (e.g Email, text messaging, etc.)". In a survey that compares three consumer segments preferences relating to the privacy boundaries for the use of eight main information technologies, among others, direct marketing tools like spam, text messaging, online advertising, Milne and Bahl (2010) report that direct marketing relies often on "opt-out" mechanism to obtain permission to use consumers information. This format is hence likely to provide more names list than the "opt-in" format that requires a prior consumers' permission, resulting in less control over personal data. Accordingly, they suggest that opt-in option is seen as granting consumers more control over personal data as a better method to build consumers' trust. As aforementioned – unpredictably – contrast to the assumption that awareness about the GDPR is likely to empower individuals with greater perceived control over their personal data, our results indicate that the awareness about the GDPR and user's empowerment are negatively

associated. This result stands in direct contrast to other prior research (Youn, 2009; Tang *et al.*, 2008; Xu *et al.*, 2012) which reported that privacy protection ensured by governmental regulations makes individuals believe that companies will protect their personal data flows, leading to a greater perceived control over their personal data. Another plausible explanation for this negative link that despite regulatory efforts to enhance consumer control over personal data, users are still misinformed about the regulations intended to regulate personal data access, processing and uses (Maier *et al.*, 2023; Kardos, 2021; Soumelidou and Tsohou, 2021). Nonetheless, this result should be interpreted with caution. In other terms, this negative link is attributable to methodological issues related to multicollinearity effects between the "awareness about the GDPR" and the awareness about the rights guaranteed by the GDPR". Note that when the item "awareness about the GDPR" was introduced alone, its effect was not statistically significant (Cf. model specification 5). This finding corroborates Bornschein *et al.* (2020) premise that asserts that experience with privacy regulation doesn't ensure alone privacy control.

Further, our empirical findings reveal that higher levels of awareness about firms and organizations practices in terms of data collections and further uses conditions are shown to be significantly associated with heightened users' privacy empowerment. This is consistent with other relevant recent research work by Luria (2023), Kumar, 2023; Maier *et al.*, (2023) that stressed the role of knowledge/awareness about digital data flows in enhancing users' control over information privacy. This finding finds also echoes in the OECD work (2013), which reports that ensuring "transparency" pertaining to personal data collection, handling, and purposes so that individuals are aware of such conditions is regarded as essential mechanism that ensures a greater control over personal data. This also mirrors findings of other prior research (Hartman-Caverly and Chisholm, 2023) that argue that the back-end implicit practices of personal data tracking and processing (such as automated decision making, inferred profiling, etc.) are often overlooked by users, resulting in loss of control over information privacy.

In addition, empirical evidence shows that users' privacy empowerment is not correlated with the following: "awareness about the right to delete data" and "awareness about the right to move data from one provider to another". A plausible explanation for a lack of significant support for this relationship might be explained by Ooijen and Vrabec (2019) work that stated that the right to data erasure should result in users' control over the scope of personal data flows. However, because of data intangibility and spread throughout the online environment, this control tends rather to lessen. Further, they claim that the right to data erasure is not an obligation when requiring a substantial effort. Furthermore, in terms of the link between perceived control and the awareness about data portability from one provider to another, the researchers asserted that because of industry monopolization, individual's control over personal data is endangered. This is as well reported by Tavani and Moor (2001). This is also in accordance with Kranenborg (2016) that advances that individuals seem simply to have no choice.

Finally, in line with the empirical results of the regression estimation, evidence revealed that user's online privacy literacy (declarative and procedural knowledge) is likely to be significantly associated with user's privacy empowerment (H3), except for the awareness and exercising the right to object receiving direct marketing, the awareness and exercising the right to delete personal data (the right to be forgotten), and the awareness about the GDPR (Cf. model specification number 4). This finding implies that despite the recent regulatory efforts to protect privacy and empower online users over personal data flows, their personal data is still jeopardized (Bornschein *et al.*, 2020, Ooijen and Vrabec, 2019). For example, the research study by Sanchez-Rola *et al.* (2019) that aimed to understand the influence of the GDPR on online users' privacy showed the ineffectiveness of data deleting/opting-out and that withdrawing consent is a mere illusion. Users' privacy empowerment should be acknowledged as a dimension of the right to data protection (Kranenborg, 2016); that is

any potential harm, whether tangible or intangible, caused by the absence of personal data protection can be mitigated by individuals' control over personal data. On the other hand, control over personal data is vital not only in terms of managing the negative consequences of data privacy threats but also to enable managing their "own" data and capitalizing on the opportunity to trade this valuable asset in the emerging market of personal data. It is believed that individuals' need for control over personal data stems essentially from the opportunity of having monetary or non-monetary compensation from data disclosure (Prince, 2018).

Conclusion, implications, limitations and future research

The main purpose of this paper is to understand the levels of OPL among EU citizens and its likely impact in strengthening online users' information privacy empowerment. Hence, the notion of OPL describes online users' information privacy awareness and skills regarding privacy protection. Reviewing recent research work related to online user privacy has revealed that empirical evidence on how privacy literacy relates to users' privacy empowerment is particularly missing. Current efforts in online privacy literature have been made to measure changes occurred on websites since the GDPR enforcement and a few other advanced studies made systematic efforts to examine levels of online privacy knowledge and skills (Ooijen and Vrabec, 2019; Bornschein *et al.*, 2020; Livingstone *et al.*, 2021; Kretschmer *et al.*, 2021; Kardos, 2021; Kumar, 2023). Yet, in most studies, little has been done to empirically assess the effect of OPL on users' information privacy empowerment, while it is crucial to understand online users' awareness about the GDPR rights/provisions and skills related to data protection and how they are likely to enhance their control over personal data, in an increasingly data-driven digital ecosystem. In summary, the lack of studies examining the effects of online privacy literacy, more particularly, the influence of awareness about GDPR provisions/rights on users' information privacy empowerment from users' perspective has been reported.

To fill this gap, this paper extends this line of the literature by empirically investigating the respective influence of two primary dimensions of online privacy literacy – namely declarative and procedural knowledge – on online users' information privacy empowerment. Specifically, we examine how users' awareness about GDPR regulation and privacy rights guaranteed by the GDPR, awareness about firms and institutions practices in terms of data collection and further uses, awareness about the existence of a public authority to report complaint against privacy violations, and the actions taken by individuals to enable them enforcing security and handling information privacy through changing the privacy settings of their personal profile from the default settings and reading privacy policy statement, are likely to enhance users' perceived control over personal data.

Our empirical results suggest that higher levels of procedural knowledge are associated with increased perceived control over personal data. From a managerial point of view, a broad implication of this finding for practitioners and E-businesses stresses the need for empowering users with greater control over their personal data through adequate privacy protecting tools to ensure more confidential transactions by placing much emphasis on cookies banners visibility (Kagan and Bekkerman, 2018; Boerman *et al.*, 2018; Bornschein *et al.*, 2020; Suh and Han, 2003). Another implication of this result is that individuals' empowerment over information privacy is often associated with a greater intention to share personal data (Prince, 2018; Kim and Kim, 2020), which is believed to be the fuel of data-driven economies and businesses that rely heavily on personal data disclosure. Hence, enhancing users' empowerment over personal information is likely to play a major role in raising users' level of personal data sharing. Furthermore, in view of our empirical results, greater awareness about firms and organizations practices in terms of data collections and further uses conditions was found to be significantly associated with

increased users' privacy empowerment. This stresses the importance of greater transparency of data tracking and processing decisions made by online businesses and services to help raise users' awareness about what type of data is monitored, used and shared and therefore providing a sense of control over their information privacy. Moreover, empirical evidence of the econometric analysis has revealed that users reporting higher levels of privacy literacy expressed higher perceived control over their personal data. From policy perspective, this finding recommends that a greater emphasis should be placed on educational and training efforts and robust privacy literacy instruction to improve users' awareness around the GDPR privacy rights and to build a sense of self-awareness about the implicit processes of data gathering and processing to enhance users' empowerment over information privacy (Hartman-Caverly and Chisholm, 2023; Maier *et al.*, 2023; Kumar, 2023; Prince *et al.*, 2023).

This study has some limitations that must be acknowledged for future research. Empirical evidence of this study shows a negative relationship between the awareness about GDPR and user's empowerment. This bears some methodological issues related to multicollinearity effects between the "awareness about the GDPR" and the "awareness about the rights guaranteed by the GDPR". Hence, to enhance the relevance of findings, we accounted for this problem in a further model estimation (Cf. model specification number 5). In addition, this research investigated the link between OPL and users' privacy empowerment using a cross-sectional survey-based research design, that does not help studying causal effects. To provide better insights regarding this link, future research needs to carry out an experimental study design to study such effects. Finally, this study is based on self-reported responses. Privacy research, however, highlights that self-assessed survey-based design is not the most relevant to assess users' privacy literacy because of social desirability and cognitive biases (Prince *et al.*, 2023; Ma and Chen, 2023). As a result, a particular caution is warranted when interpreting the results of this paper. Therefore, in future studies, an experimental research design is warranted to better assess the relevance of our research findings. Further, our study restricts the analysis of the effects of OPL on users' empowerment over personal information privacy to the population of EU citizens, which is likely to pose generalizability problems. This stresses the need to extend this work to a broader population of non-European countries while considering Internet users' awareness of regulations and policies related to personal information privacy when studying the online privacy literacy.

References

Alshibly, H. and Chiong, R. (2015), "Customer empowerment: does it influence electronic government success? A citizen-centric perspective", *Electronic Commerce Research and Applications*, Vol. 14 No. 6, pp. 393-404, doi: 10.1016/j.elerap.2015.05.003.

Arachchilage, N.A. and Love, S. (2014), "Security awareness of computer users: a phishing threat avoidance perspective", *Computer Human Behavior*, Vol. 38 No. 38, pp. 304-312, doi: 10.1016/j.chb.2014.05.046.

Bartsch, M. and Dienlin, T. (2016), "Control your Facebook: an analysis of online privacy literacy", *Computers in Human Behavior*, Vol. 56, pp. 147-154, doi: 10.1016/j.chb.2015.11.022.

Boerman, S.C., Kruikemeier, S. and Zuiderveen Borgesius, F.J. (2018), "Exploring motivations for online privacy protection behavior: insights from panel data", *Communication Research*, Vol. 48 No. 7, pp. 1-25, doi: 10.1177/0093650218800915.

Bornschein, R., Schmidt, L. and Maier, E. (2020), "The Effect of consumers' perceived power and risk in digital information privacy: the example of cookie notices", *Journal of Public Policy and Marketing*, Vol. 39 No. 2, pp. 1-20, doi: 10.1177/0743915620902143.

Borooah, V.K. (2002), *Logit and Probit: Ordered And Multinomial Models, Quantitative Applications in the Social Sciences*, Sage Publication, Thousand Oaks, CA.

CongerPratt, S.J.H. and Loch, K.D. (2012), "Personal information privacy and emerging technologies", *Information Systems Journal*, Vol. 25 No. 5, pp. 401-417, doi: 10.1111/j.1365-2575.2012.00402.x.

Correia, J. and Compeau, D. (2017), "Information privacy awareness (IPA): a review of the use, definiation and measurement of IPA", *Proceedings of the 50th Hawaii International Conference on System Sciences*, pp. 4021-4030.

Debatin, B., Lovejoy, J.P., Horn, A. and Hughes, B.N. (2009), "Facebook and online privacy: attitudes, behaviors, and unintended consequences", *Journal of Computer Mediated Communication*, Vol. 15 No. 1, pp. 83-108, doi: 10.1111/j.1083-6101.2009.01494.x.

Demmers, J., Van Dolen, W.M. and Weltevreden, J.W.J. (2018), "Handling consumer messages on social networking sites: customer service or privacy infringement?", *International Journal of Electronic Commerce*, Vol. 22 No. 1, pp. 8-35, doi: 10.1080/10864415.2018.1396110.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Research Systems*, Vol. 1 No. 7:1, pp. 61-80, doi: 10.1287/isre.1060.0080.

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. and Sadeh, N. (2017), "Privacy expectations and preferences in an IoT world", *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS'17)*.

Gerlach, J.P., Eling, N., Wessels, N. and Buxmann, P. (2018), "Flamingos on a slackline: companies' challenges of balancing the competing demands of handling customer information and privacy", *Information Systems Journal*, Vol. 29 No. 2, pp. 548-575, doi: 10.1111/isj.12222.

Gordon, S. (2018), "Our personal data are precious—we must take back control", in *Power and Big Tech, 2017*, [Online]. available at: https://www.ft.com/content/3278e6dc-67af-11e7-9a66-93fb352ba1fe (accessed 12 April 2018).

Guadagni, P.M. and Little, J.D.C. (1983), "A logit model of brand choice calibrated on scanner data", *Marketing Science*, Vol. 3 No. 2, pp. 208-238.

Hagendorff, T. (2018), "Privacy literacy and its problems", *Journal of Information Ethics*, Vol. 27, p. 127.

Hargittai, E. and Litt, E. (2013), "New strategies for employment? Internet skills and online privacy practices during people's job search", *IEEE Security and Privacy*, Vol. 11 No. 3, pp. 38-45, doi: 10.1109/msp.2013.64.

Hartman-Caverly, S. and Chisholm, A.E. (2023), "Privacy as Respect for Persons: Reimagining Privacy Literacy with the Six Private I's Privacy Conceptual Framework".

Kagan, S. and Bekkerman, R. (2018), "Predicting purchase behavior of website audiences", *International Journal of Electronic Commerce*, Vol. 22 No. 4, pp. 510-539, doi: 10.1080/10864415.2018.1485084.

Kardos, V. (2021), "Privacy literacy and the protection of personal data in the mind of law students", *Public Administration*, Vol. 4, pp. 124-141, doi: 10.32575/ppb.2021.4.8.

Kim, B. and Kim, D. (2020), "Understanding the key antecedents of users' disclosing behaviors on social networking sites: the privacy paradox in sustainability", [Online]. available at: https://mdpi-res.com/d_attachment/sustainability/sustainability-12-05163/article_deploy/sustainability-12-05163-v2.pdf?version=1593120597 (Accessed 20 April 2021).

KortesniemiLagutinElo, Y.D.T., Fotiou, N. and Fotiou, N. (2019), "Improving the privacy of IoT with decentralised identifiers (DIDs)", *Journal of Computer Networks and Communications*, Vol. 2019, pp. 1-10, doi: 10.1155/2019/8706760.

Kranenborg, H. (2016), *O. Lynskey,the Foundations of EU Data Protection Law*, International Data Privacy Law in Oxford University Press, Oxford.

Kretschmer, M., Pennekamp, J. and Wehrle, K. (2021), "Cookie banners and privacy policies: Measuring the impact of the GDPR on the web", *ACM Transactions on the Web (TWEB)*, Vol. 15 No. 4, pp. 1-42.

Kumar, P.C. (2023), "What is privacy literacy for?", *In proceedings of the 23rdAnnual Conference of the Association of Internet Researchers*, Dublin, Ireland, AoIR.

Li, H., Sarathy, R. and Xu, H. (2011), "The role of affect and cognition on online consumers' willingness to disclose personal information", *Decisions Support System*, Vol. 51 No. 3, pp. 434-445, doi: 10.1016/j.dss.2011.01.017.

Linden, T., Khandelwal, R., Harkous, H. and Fawaz, K. (2018), *"The privacy policy landscape after the GDPR", arXiv preprint arXiv:1809.08396*.

Livingstone, S., Stoilova, M. and Nandagiri, R. (2021), "Data and privacy literacy: the role of the School in educating children in a datafied society", in *The Handbook of Media Education Research*, pp. 413-425.

Luria, M. (2023), "Co-design perspectives on algorithm transparency reporting: guidelines and prototypes", *In proceedings of ACM Conference on Fairness, Accountability, and Transparency*, pp. 1076-1087.

MaChen, S.C. (2023), "Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior", *Frontiers in Psychology*, Vol. 14, 1224168, doi: 10.3389/fpsyg.2023.1224168.

Maier, E., Doerk, M., Reimer, U. and Baldauf, M. (2023), "Digital natives aren't concerned much about privacy, are they?", *I-Com*, Vol. 22 No. 22: 1, pp. 83-98, doi: 10.1515/icom-2022-0041.

Massara, F., Raggiotto, F. and Voss, W.G. (2021), "Unpacking the privacy paradox of consumers: a psychological perspective", *Psychology and Marketing*, Vol. 38 No. 10, pp. 1814-1827, doi: 10.1002/mar.21524.

Masur, P.K. (2020), "How online privacy literacy supports self-data protection and self-determination in the age of information", *Media Communication*, Vol. 8 No. 2, pp. 258-269, doi: 10.17645/mac.v8i2.2855.

Masur, P.K., Teutsch, D. and Trepte, S. (2017), *Entwicklung und Validierung der Online-Privatheits-Kompetenzskala (OPLIS) [Development and Validation of The Online Privacy Literacy Scale (OPLIS)]*, Hogrefe Verlag, Diagnostica, pp. 256-268.

Masur, P.K., Hagendorff, T. and Trepte, S. (2023), "Challenges in studying social media privacy literacy", in *The Routledge Handbook of Privacy and Social Media*, Tylor and Francis Group.

Midha, V. (2012), "Impact of consumer empowerment on online trust: an examination across genders", *Decision Support Systems*, Vol. 54 No. 1, pp. 98-205, doi: 10.1016/j.dss.2012.05.005.

Milne, G.R. and Bahl, S. (2010), "Are there differences between consumers' and marketers' privacy expectations? A segment- and technology-level analysis", *Journal of Public Policy & Marketing*, Vol. 29 No. 1, pp. 138-149, doi: 10.1509/jppm.29.1.138.

Moran, N. (2020), "Illusion of safety: how consumers underestimate manipulation and deception in online, (vs. Offline) shopping contexts", *Journal of Consumer Affairs*, Vol. 54 No. 3, pp. 890-911, doi: 10.1111/joca.12313.

OECD (2013), "OECD guidelines on the protection of privacy and transborder flows of personal data", in [Online]. available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 2 March 2017).

Ooijen, I. and Vrabec, H.U. (2019), "Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective", *Journal of Consumer Policy*, Vol. 42 No. 1, pp. 91-107, Springer, doi: 10.1007/s10603-018-9399-7.

Park, Y.J. and Jang, S.M. (2014), "Understanding privacy knowledge and skill in mobile communication", *Computers in Human Behavior*, Vol. 38, pp. 296-303, doi: 10.1016/j.chb.2014.05.041.

Pingo, Z. and Narayan, B. (2017), "*Privacy literacy: extending information literacy in the age of social media and big data*", *i3 Information Interactions and Impact*.

Prince, C. (2018), "Do consumers want to control their personal data? Empirical evidence", *International Journal of Human-Computer Studies*, Vol. 110, pp. 21-32, doi: 10.1016/j.ijhcs.2017.10.003.

Prince, C., Omrani, N., Maalaoui, A., Dabic, M. and Kraus, S. (2023), "Are we living in `Surveillance societies and is privacy an illusion? An empirical study on privacy literacy and privacy concerns", *IEEE Transactions on Engineering Management*, Vol. 70 No. 10, pp. 3553-3570, doi: 10.1109/TEM.2021.3092702.

Robinson, E.P. and Zhu, Y. (2020), "Beyond 'I agree': users' understanding of web site terms of service", *Social Media Society*, Vol. 6 No. 1, 2056305119897321, doi: 10.1177/2056305119897321.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, M., Balzarotti, D., Bilge, L., Vervier, P.-A. and Santos, I. (2019), "Can I opt out yet? GDPR and the global illusion of cookie control", *In ACM Asia Conference on Computer and Communications Security (AsiaCCS '19)*, July 9-12, 2019, ACM, Auckland, New Zealand, New York, NY, USA, 12 pages.

Sindermann, C., Schmitt, H.S., Kargl, F., Herbert, C. and Montag, C. (2021), "Online privacy literacy and online privacy behavior – the role of crystallized intelligence and personality", *International Journal of Human–Computer Interaction*, Vol. 37 No. 15, pp. 1455-1466, doi: 10.1080/10447318.2021.1894799.

Soumelidou, A. and Tsohou, A. (2021), "Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness", *Telematics and Informatics*, Vol. 61, 101592, doi: 10.1016/j.tele.2021.101592.

Suh, B. and Han, I. (2003), "The impact of customer trust and perception of security control on the acceptance of electronic commerce", *International Journal of Electronic Commerce*, Vol. 7 No. 3, pp. 135-161.

Tang, Z., Hu, Y.J. and Smith, M.D. (2008), "Gaining trust through online privacy protection: self-regulation, mandatory standards, or caveat emptor", *Journal of Management Information Systems*, Vol. 2 No. 4:4, pp. 153-173, doi: 10.2753/mis0742-1222240406.

Tavani, H.T. and Moor, J.H. (2001), "Privacy protection, control of information, and privacy-enhancing technologies", *Computer and Society*, Vol. 31 No. 1, pp. 6-11, doi: 10.1145/572277.572278.

Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M. and Hennhöfer, A. (2015), "Do people know about privacy and data protection strategies? Towards the Online Privacy Literacy Scale", (OPLIS), in Gulwirth, S., Leenes, R. and Hert, P. (Eds), *Reforming European Data Protection Law*, Springer, pp. 333-365.

Urban, T., Degeling, M., Holz, T. and Pohlmann, N. (2019), "Your hashed IP address: ubuntu. Perspectives on transparency tools for online advertising", *2019 Annual Computer Security Applications Conference (ACSAC '19)*, San Juan, PR, USA, December 9-13, 2019, ACM, New York,NY, USA, 16 pages.

Urban, T., Tatang, D., Degeling, M., Holz, T. and Pohlmann, N. (2020), "Measuring the impact of the GDPR on data sharing in Ad networks", *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20)*, Taipei, Taiwan, June 1-5, 2020, ACM, New York, NY, USA, 14 pages.

Van Dyke, T.P., Midha, V. and Nemati, H. (2007), "The effect of consumer privacy empowerment on trust and privacy concerns in E-Commerce", *Electronic Markets*, Vol. 17 No. 1, pp. 68-81, doi: 10.1080/10196780601136997.

Weinberger, M., Zhitomirsky-Geffet, M. and Bouhnik, D. (2017), "Factors affecting users' online privacy literacy among students in Israel", *Online Information Review*, Vol. 41 No. 5, pp. 655-671, doi: 10.1108/oir-05-2016-0127.

Wissinger, C.L. (2017), "Privacy literacy: from theory to practice", *Communications in Information Literacy*, Vol. 11 No. 2, pp. 378-389, doi: 10.15760/comminfolit.2017.11.2.9.

Xu, H., Teo, H.H., Tan, B.C.Y. and Agarwal, R. (2012), "Research note-effects of individual self-protection, industry, self-regulation, and government regulation on privacy concerns: a study of

location-based services", *Information Systems Research*, Vol. 23 No. 4, pp. 1342-1363, doi: 10.1287/isre.1120.0416.

Youn, S. (2009), "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents", *Journal of Consumer Affairs*, Vol. 43 No. 3, pp. 389-418, doi: 10.1111/j.1745-6606.2009.01146.x.

About the authors

Christine Prince is Associate Professor of Marketing at the ISG International Business School, Paris. She received a Ph.D. degree in Business Administration with Specialization in Marketing Management at the University of Paris 11, France. Her primary research interests involve online consumer behavior, online privacy, privacy literacy and quantitative marketing.

Nessrine Omrani is Full Professor of Digital Transformation and the Director of Management Department at Paris School of Business. She holds a Ph.D. degree in Economics from the University of Paris-Saclay and a post-doctoral degree (HDR) in Management from the University of Paris-Est. She has publications in various academic journals, such as the *Journal of Economic Literature*, *Technological Forecasting and Social Change*, *IEEE Transactions on Engineering Management*, *Information Economics and Policy*, the *European Journal of Comparative Economics* and *Economic and Industrial Democracy*. Her research interests include the areas of digital transformation, online consumer behavior, crowdfunding and privacy.

Francesco Schiavone is Full Professor of Management at Parthenope University of Naples, Italy. He received his Ph.D. degree in Network Economics and Knowledge Management from the Ca' Foscari University of Venice (Italy) in 2006. He is also Adjunct Professor at EM Lyon and Paris School of Business (France). Currently, his main research areas are technology management, strategic innovation and healthcare management and innovation. He has published in numerous international journals such as the *Journal of Business Research*, the *European Management Journal*, *European Management Review*, the *European Journal of Innovation Management*, the *International Journal of Innovation Management*, the *Journal of Intellectual Capital*, the *Journal of Knowledge Management*, *Technology Analysis and Strategic Management* and *Technological Forecasting and Social Change*, among others. Francesco Schiavone is the corresponding author and can be contacted at: franz.schiavone@gmail.com