Italian Journal of Marketing (2020) 2020:309–342
https://doi.org/10.1007/s43039-020-00017-2

ORIGINAL ARTICLE

Hands off my data: users' security concerns and intention to adopt privacy enhancing technologies

Federico Mangiò[1] · Daniela Andreini[1] · Giuseppe Pedeliento[1]

Received: 3 October 2020 / Accepted: 16 November 2020 / Published online: 22 November 2020

Abstract

As the number of data leak scandals and data infringements increase by the day, people are becoming more concerned than ever about their online security. As a result, software and applications designed to reduce, eliminate, or prevent unauthorized processing of users' online personal data, referred to as privacy enhancing technologies (PETs) are gaining momentum. Yet, research investigating what drives users' intention to adopt these technologies is still scant. Drawing on the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2), this study develops a research framework and tests it with a research design combining structural equation modelling and multi-group analysis. As participants, we recruited 198 members of four online communities where discussion of PETs takes place. Besides confirming the UTAUT2 variables' predictive power on the intention to use PETs, the results of applying the baseline model also provide interesting insight on the mediating role UTAUT2 core constructs play in the relationship between security concerns and intention to adopt PETs. The multi-group analysis, in contrast, revealed that the underlying mechanisms of the theoretical framework we tested work differently when the users' level of expertise is taken into account. This work concludes with managerial implications addressed to both PET providers and any business dealing with online consumer data.

Keywords Privacy enhancing technologies (PET) · Security concerns · Hedonic motivations · Social influence · SEM

✉ Federico Mangiò
federico.mangio@unibg.it

Daniela Andreini
daniela.andreini@unibg.it

Giuseppe Pedeliento
giuseppe.pedeliento@unibg.it

[1] Department of Management, University of Bergamo, Via dei Caniana 2, 24127 Bergamo, Italy

1 Introduction

In the aftermath of age-marking data leak scandals and in the midst of recurrent data breaches, people appear to be more concerned than ever about the benefits of staying anonymous online (Anant et al. 2020). According to a recent study the large majority of internet users do have security concerns, i.e. they fear possible breaches of their personal data (NortonLifeLock 2020). Current statistics show that such concerns are amply justified as the number of recorded data breaches have skyrocketed in the past few years, going from 157 in 2015 to 1473 in 2019 (Identity Theft Resource Center 2020).

Not only are people trying to protect their personal data from online criminal attacks; increasingly, they are also aspiring to online anonymity, i.e. to be able to surf the web anonymously by completely or partially concealing their identity (Morio and Buchholz 2009; Wallace 2008; Pfitzmann and Köhntopp 2001; Marx 1999).

Desiring anonymity is often stigmatized (Gehl 2016)—frequently by being associated with mean and harmful behavior, such as cyberbullying (Barlett and Gentile 2012), illegal file-sharing (Larsson et al. 2012), and illegal or unethical trade (Morselli et al. 2017). However, online anonymity is a condition coveted by many more than just criminals and wrongdoers.

Since global supremacy has been achieved and established by internet giants (Weiss et al. 2004) such as Facebook, Instagram, Google, and Amazon, issues of online anonymity have become popular and gained wide political, economic, social, academic, and media traction. This is due to the requirement that for such companies to exist and thrive, users' identities be displayed and their online activities and behaviors be tracked (Zuboff 2015, 2019; Gehl 2016; Stryker 2012; Galperin 2011). Thus, online anonymity has become an ideological struggle and a mindful choice people make to purposefully contest internet players' invasive, manipulative, and surveilling marketing practices (Zuboff 2015, 2019; Clarke 2019; West 2019; Gehl 2016; Jardine 2016; Maddox et al. 2016).

As a consequence, gaining a deeper understanding of how consumers' online security concerns can materially hinder such practices and therefore threaten the long-lasting survival of ever more data-hungry business models is paramount and cannot be procrastinated any further.

On these premises, it is no wonder that the market of the so called 'Privacy Enhancing Technologies (PET), i.e. a wide and heterogeneous family of information and communication technologies (ICTs) designed to reduce, eliminate, or prevent unauthorized processing of users' personal data to protect their privacy and security (Heurix et al. 2015; Borking and Raab 2001) such as proxy servers, virtual private networks (VPNs), end-to-end secure communications, and anonymization networks like The Onion Router (known as Tor), have recently gained momentum (Kaaniche et al. 2020; Sardá et al. 2019).

Although most of the available technologies are still very hard for ordinary Internet users to master (Shelton et al. 2015; Kang et al. 2013; Borking 2011; Roßnagel 2010), others that are easier to use are becoming popular and their penetration is constantly increasing, both on the demand side (e.g. GlobalWebIndex 2018a) and on the supply side (e.g. Global Market Insights 2020).

Yet, the market hype for these new technologies has not produced an equal hype in user-focused research. A careful analysis of current literature dealing with online anonymizers (reported below) reveals that extant research focuses largely on these technologies' technical features, and overlooks the role of the users and their use behaviors. As Harborth et al. (2020) have recently stated, despite acceptance that PETs' wide penetration is tightly connected to a deep understanding of usage behavior, literature to build such understanding is still very scant. In addition, the few studies available to date expose at least three other important research gaps. First, they are generally focused on the specific characteristics that make particular PETs the sole drivers in determining users adopt them. Second, they underestimate intrinsic motivations, as well as others' influence in prompting users to adopt PETs despite these additional motives often having been demonstrated as paramount in driving other technologies' use (Shaw and Sergueeva 2019; Alalwan et al. 2017; Herrero and San Martín 2017; Morosan and De Franco 2016; Slade et al. 2015). Third, and most important, despite PET enhancing both online privacy and security (Gan, et al. 2019) and despite users' concerns about their personal data security is a crucial aspect in fostering the adoption of these technologies (Acquisti and Grossklags 2005; Belanger et al. 2002; Hoffman et al. 1999; Reiter and Rubin 1998), previous research has only focused on privacy concerns while overlooking security concerns.

Acknowledging these gaps, this research answers the following research question: How do users' concerns for their personal data security affect their intention to adopt PETs? To provide an answer to this question we develop a theoretical framework which combines the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) (Venkatesh et al. 2012) with literature on users' attitude towards personal data (Addae et al. 2017) and we test it in a representative consumer-driven community context.

This paper is structured as follows: First it reviews the relevant literature on PETs, based on which it develops the theoretical model and provides justification for the tested hypotheses. This is followed by a methodological section in which we provide information about the research context and give details about the data gathering procedure and the analytical method we used. Finally, we present the findings, a general discussion of the results, the implications, the study's limitations, and some concluding remarks.

2 Literature review

The term Privacy Enhancing Technology (PET) covers a broad range of technologies and applications that are designed to enhance privacy and data security of both individual (e.g. Kaaniche et al. 2020) and corporate users (e.g. Gan et al. 2019) in their online activities and communications. There are multiple technologies that can be grouped together under the PET label. On the end-user side, in particular, these range from end-to-end secure messaging tools, Virtual Private Networks (VPNs), to anonymization networks and anti-tracking software (ENISA 2016). In particular, communication anonymizers, i.e. online anonymity-granting software and applications, are among the most important users-oriented PETs in circulation (Nia and Martinez 2018; Spiekermann 2005). Despite PETs being as old as the web itself (Fritsch 2007), research has largely focused on their technical features while the role of users has been overlooked (Harborth et al. 2020). As a matter of fact, looking closely at the literature to date reveals three separate research branches in studies on PETs. First, there are studies connected to the branch of economic research, which brings together work aimed at making sense of the PET market's evolutionary dynamics and at identifying the main technological and economic barriers to the wide diffusion of these technologies (e.g. Caulfield et al. 2016; Borking 2011; Roßnagel 2010; Acquisti 2004; Feigenbaum et al. 2002). Second, connected to the branch of ICT and information system research, there are studies adopting a highly-tech and PET-specific focus meant to evaluate the PET and to illustrate the technical enhancements that can improve their usability and their effectiveness (e.g. AlSabah and Goldberg 2016; Norcie et al. 2012; Fabian et al. 2010; Clark et al. 2007; Whitten and Tygar 1999). Third, connected to the tradition of information system research focused on the end-user, there is a set of studies that try to shed light on the user's perspective on adopting such technologies. Compared to the first two research streams, this third one is still in its infancy and therefore comparatively smaller. Namara et al. (2020) and Harborth et al. (2020) recently mentioned how surprising it is that empirical research on what motivates users to adopt PETs is still underdeveloped, considering their overall service quality and cost-effectiveness, which dramatically depends on the degree of diffusion they are able to achieve. The few available publications that explain users' adoption of PETs (or intention to adopt them) have relied on the Technology Acceptance Model (TAM) (Davis 1985) (see Table 1 for an overview), extending this pioneering theory on why people do or do not use technologies, to encompass variables suited to measuring users' perceptions of PET-specific attributes. These studies include attention to users' perception of the anonymizer's ability to grant anonymity (Harborth et al. 2020), users' feelings of trust toward the technology (Benenson et al. 2014; Krontiris et al. 2015; Harborth et al. 2020), users' perceived risks (Krontiris et al. 2015), users' perception of being well informed about how PETs function (Benenson et al. 2014; Krontiris et al. 2015), and users' awareness of or concerns about their online privacy (Brecht et al. 2011, 2012; Benenson et al. 2014). However, despite the TAM undoubtedly being the most widely used framework to assess users' actual adoption or intention to adopt certain technologies (see Legris et al. 2003; Turner et al. 2010; Marangunić and Granić 2015 for a review of previous applications of the TAM), it is limited to a small number of variables, mostly perceived ease of use and perceived usefulness, and does not include any variable related to the user-technology interface that can affect the decision to use a technological aid, or not. Therefore, the TAM needs to be adapted and modified to fit the peculiar technical and use-based conditions that might limit or foster the use of technologies (Pizzi and Scarpi 2020; Marangunić and Granić 2015). The result of most recent research being theoretically based on the few variables composing the TAM is that the literature offers just a partial understanding of what determines users' decisions to turn to PETs. Despite scholars confirming that the decision to use PETs can be influenced by both subjective and social

Table 1 An overview of previous users-focused research on PET adoption

Author	Method	Theoretical background	Sample	PET	Precursors to usage	Findings
Harborth et al. (2020)	Mixed: survey and qualitative analysis of open-ended questions	TAM	256 users	Tor, JonDonym	Perceived anonymity, trust in the service, perceived usefulness, perceived ease of use.	The TAM, extended with the proposed additional constructs, explains more than 50% of the variance of the users' intention to use the PETs investigated
Namara et al. (2020)	Mixed: survey and IDI	TAM combined with risk-as-a-feeling theory (Lowenstein et al. 2001)	90 tech-savvy informants and 5 actual VPN users	VPN	Cognitive evaluations, emotional considerations, external stimuli	Users who are mainly moved by emotional considerations (e.g. fear of surveillance, privacy concerns) tend to sustain PET adoption over time, whilst those moved by cognitive evaluations (e.g., practical motivations and technical purposes) tend to abandon the PET

Table 1 (continued)

Author	Method	Theoretical background	Sample	PET	Precursors to usage	Findings
Harborth and Pape (2018, 2019)	Quantitative survey	IUIPC (Malhotra et al. 2004)	141 users and 124 users	Tor, JonDonym	IUIPC, trusting beliefs in the PET	IUIPC negatively affects trusting beliefs and positively affects risk beliefs and trusting beliefs in the PET; trusting beliefs in turn have a negative effect on risk beliefs; trusting beliefs in the PET positively affects the actual use of PET, whilst the effect of trusting beliefs and risk beliefs is not statistically significant

Table 1 (continued)

Author	Method	Theoretical background	Sample	PET	Precursors to usage	Findings
Krontiris et al. (2015), Benenson et al. (2014, 2015)	Quantitative survey	TAM	30 users 41 computer science students	Privacy attribute-based credentials ABC)	Perceived usefulness for the primary/secondary task, perceived ease of use, trust in the service, perceived risk, situation awareness, perceived anonymity, understanding of the PET	Even though sample size is too restricted to infer and generalize significant results, from explorative analysis the authors suggest that core TAM's constructs (perceived usefulness, perceived ease of use) can play an important role in affecting users' PET adoption; similarly, the service usability and the user's understanding of the specific PET play a role. Trust in the service seems to be independent of user's actual understanding of the PET

Table 1 (continued)

Author	Method	Theoretical background	Sample	PET	Precursors to usage	Findings
Brecht et al. (2011, 2012)	Quantitative survey Lab experiment	TAM combined with big five personality traits (McCrae and John 1992)	1111 participants (only 4% users) 151 students	Tor Tor, I2P, Java Anon Proxy, VPN, anonymous remailers	Actual vs stated internet literacy, privacy awareness, internet privacy concerns, internet patience, Big Five personality traits, perceived usefulness	Individual internet literacy, privacy concerns, and internet privacy awareness affect the users' intention to adopt PETs. Perceived usefulness significantly mediates these relationships. While browsing anonymously, users accept a longer waiting time compared to traditional browsing. Regarding the effects of personality traits, only openness leads to higher probability to adopt PETs, whilst neuroticism is found to exert a significant effect on privacy concerns. Actual internet privacy literacy negatively affects privacy awareness, whilst stated internet privacy literacy has an opposite effect

motives, research to date has rarely taken these sources of influence into account. One exception, for example, is Brecht et al. (2011, 2012) who intended to give more centrality to the user than the technology. They used the TAM in tandem with users' personality traits (McCrae and John 1992), i.e. extroversion, agreeableness, conscientiousness, neuroticism, and openness to experience, as possible determinants of users' intention to use PETs. Further, Harborth and Pape (2018, 2019), turned to Malhotra et al. (2004) Internet Users Information Privacy Concerns model, that, different to the TAM, includes variables measuring privacy concerns, as well as determinants of such concerns, such as trust and risk beliefs. Namara et al. (2020), in contrast, shed light on some non-utilitarian reasons for users' decisions to use PETs. In a study based on a sample of VPN users, they found that emotional considerations, such as the strong desire to protect online privacy or fear of surveillance and data tracking, are more likely to explain users' PET adoption over time than practical-technical considerations (such as technology usefulness and usability).

Besides the inadequacy of the theoretical frameworks that have mostly been used in current research, the literature to date reports studies focusing on users' privacy concerns as a reason for adopting PETs (Harborth and Pape 2019; Brecht et al. 2011, 2012), while they neglect security concerns, despite online anonymizers allow users to satisfy both these concerns (Gan et al. 2019). Although privacy concerns could be mistaken for security concerns, and vice versa, they are two different concepts that respond to two different needs (Belanger et al. 2002). Privacy concerns relate to the users' fear that their data and personal information can be disclosed to unauthorized parties (Chellappa 2008). Security concerns, however, relate to individual perceptions of how relevant and adequate existing technical and legal protective measures are to ensure integrity, confidentiality, and reliability of personal data (Addae et al. 2017). Clearly, the protection of privacy does not necessarily guarantee the protection of security, nor the other way around. For example, the two-factor identification used in home banking services makes transactions more secure, but keeps the identity of the user visible to the bank service provider. The possibility for Facebook users to prohibit others tagging them in pictures is a functionality considered to protect users' privacy, but it has not affected the security of users' social profiles. In fact, research has disclosed that users are often willing to sacrifice a part of their privacy in exchange for a higher level of security, and vice versa (Norberg et al. 2007; Dinev and Harth 2006; Acquisti 2004; Culnan and Bies 2003). PETs, however, although primarily designed to achieve anonymity, do also provide higher levels of security. Notably, providers of anonymity-granting technologies emphasize these tools' ability to protect both privacy and security online (Khan et al. 2018).

Considering the above, our study acknowledges a substantial lack of studies focused on understanding what leads users to adopt PETs or not, also due to the inadequacy of the theoretical tools applied. The study additionally notes a lack of research focused on users' security concerns as a PET adoption driver. This research draws on a compelling theory of technology adoption (the UTAUT2, Venkatesh et al. 2012) and tests a set of hypotheses coherent with this theoretical device. The following section describes and further reports on the hypotheses developed and tested.

3 Theoretical framework and development of the hypotheses

3.1 Modelling technology acceptance: from TAM to UTAUT2

Research on acceptance and use of technologies has flourished in the last few decades. Scholars have developed, tested, and validated several models to explain why individuals intend or actually do use technological aids such as the above-mentioned TAM (Davis 1985). Being the TAM based on the principal tenets of the Theory of Reasoned Action (Fishbein 1979) and despite being originally conceived to predict users' acceptance of IS technologies in organizational settings, the TAM has been extensively used to study the adoption of various technologies also in consumer settings, both offline and online (e.g. Lin and Kim 2016; Ha and Stoel 2009; Pizzi and Scarpi 2020). In brief, the TAM postulates that users' adoption of technology is determined by their attitude towards the technology which, in turn, is affected by the usefulness and the perceived ease-of-use of the technology. The parsimonious nature of the TAM made this model suitable for multiple applications in heterogenous contexts, however it has also been recognized as a constraining drawback which lead some researchers to extend the baseline TAM framework (see e.g. Pizzi and Scarpi 2020). Consistent with these critiques, Venkatesh et al. (2003) developed a unified theory of acceptance and use of technology (UTAUT) suited to explain technology adoption in the organizational setting, which supplemented the TAM. The original formulation of the UTAUT was then followed by the UTAUT 2 (Venkatesh et al. 2012) which, although keeping the theoretical premises of the UTAUT, includes an additional set of variables to make it applicable to the wide range of technologies that are used for non-work-related reasons. The latter technologies, hence, can also be fruitfully applied to the specific case of PET that, despite originally being designed for organizations, are now more often applied by individual internet users (Namara et al. 2020). The UTAUT2 incorporates explanatory variables which simultaneously regard the technical sphere, the user's intrinsic motivations, and the surrounding social context. For these reasons, the UTAUT2 has extensively proved to be well suited to explain adoption of technological applications in online as well as in mobile settings (Shaw and Sergueeva 2019; Alalwan et al. 2017; Herrero and San Martín 2017; Morosan and De Franco 2016; Slade et al. 2015). In detail, the UTAUT2 assumes that intention to use and actual use of a technology depend on seven main precursors: *performance expectancy*, *effort expectancy*, *social influence*, *facilitating conditions* (which are all included in the UTAUT), *hedonic motivation*, *price value,* and *habit* (which are UTAUT2 extensions). In particular, *performance expectancy* and *effort expectancy,* respectively, refer to the "degree to which using a technology will provide benefits to consumers in performing certain activities" and the "degree of ease associated with consumers' use of technology" (Venkatesh et al 2012, p. 159). These predictive variables are particularly important in the realm of PETs. These technologies, in fact, tend to be difficult to assess in terms of actual performance (Roßnagel 2010), are in many cases not particularly user-friendly (Roßnagel 2010; Galletta et al. 2004), and are often difficult for consumers to install and configure (Lee et al. 2017). Different to *performance* and *effort expectancy*, which cover the technical benefits that the use of a technology brings to its users, the construct of *social influence* relates to the presence and the impact of social forces in fostering or limiting the adoption of a technology, i.e. "the extent to which consumers perceive that important others (e.g. family and friends) believe they should use a particular technology" (Venkatesh et al. 2012, p. 159). In the case of PETs these social influences have been found and suggested to foster the decision to adopt and use the technologies. Besides appreciating PETs' technical qualities, users increasingly value and seek online anonymity as a form of consumers' antagonism to the so-called 'surveillance capitalism' (Zuboff 2015, 2019) which has thick subcultural overtones. As such, using PET is now often framed as a way of signifying one's membership of groups and collectives that through actions resist firms and organizations suspected of using personal data and information for their own profit. As the UTAUT model was originally developed to explain technology adoption in the organizational setting, researchers included *facilitating conditions* to assess the degree to which an individual believes an organizational and technical infrastructure exists to support them using the system (Venkatesh et al. 2003). Hence, the construct of facilitating conditions, when applied to technologies used for private, i.e. non-organizational, purposes, is equated to the construct of perceived behavioral control found in the theory of planned behavior (Ajzen 1991), or to the construct of self-efficacy in Bandura's social learning theory (Bandura et al. 1999). This construct, in fact, refers to the person's belief that he/she is in control of the behavior in question, such as using a technology (Venkatesh et al. 2003).

In addition to these four drivers that prompt technology adoption, i.e. *performance expectancy*, *effort expectancy*, *social influence*, *facilitating conditions*, Venkatesh et al.'s (2012) UTAUT2 model adds three more drivers, namely *hedonic motivation*, *price value,* and *habit*. *Hedonic motivation*, which was added to the original formulation of the UTAUT to account for intrinsic and affective motivations in predicting consumer technology adoption, refers to "the fun or pleasure derived from using a technology" (Venkatesh et al. 2012, p. 161). In a recent review of this construct's complex introduction to UTAUT2-based studies, Tamilmani et al. (2019) found that the large majority of studies supported a significant effect of hedonic motivations on the behavioral intention to adopt a technology.

Using online anonymizers and PETs in general can be fun and entertaining for the end-user (Kang et al. 2013). The use of these technologies in fact requires users to continuously experiment with new tools, to update the existing ones, and interact with other users for problem solving during anonymous navigation or simply to improve enjoyment of the anonymous experience. *Price value* assesses the consumers' cognitive trade-off between the perceived benefits of the technology and the monetary costs associated with purchasing and using it. Finally, *habit* refers to the extent to which people tend to perform behaviors automatically. As Venkatesh et al. (2003) noted, habit should be included as use behavior does not necessarily result from deliberated decisions, but can be a part of taken for granted routines and habits. As with other models designed to explain the phenomenon of technology adoption, the seven constructs composing the full UTAUT2 have rarely all been included in a single empirical study. A recent meta-analysis of empirical research grounded on the UTAUT2 tenets (see Tamilmani et al. 2018a, b), revealed that more than sixty percent of the published studies did not include the *habit* and the *price value* construct, and those that did, quite often reported inconsistent effects. Specifically, *habit* is often excluded in studies referring to new technology and when users are at an early stage of adoption, i.e. before sufficient time has elapsed for users to form a habit in using it (Tamilmani et al. 2018a, b). The variable of *price value,* in contrast, is excluded because the vast majority of the technologies we investigated do not require any kind of financial contribution from the user. Similarly, since this research focuses on newly established technologies and since it focuses of technologies available to users for free, e.g. Tor or the majority of popular personal VPNs and proxy servers, we excluded the constructs of habit and of price value in developing the framework and its underlying hypotheses. Based on this reasoning we advance the following hypothesis:

H1 Performance expectancy (H1a), effort expectancy (H1b), social influence (H1c), facilitating conditions (H1d), and hedonic motivation (H1e) directly and positively influence users' intention to adopt PETs.

3.2 Security concerns

A main reason for users wanting PETs is to protect their online anonymity, i.e. to avoid others, such as internet service providers, websites, or social networks to link online behavior to their identity. PETs give users two main benefits related to anonymity: privacy and security. Privacy, refers to individuals' right to determine for themselves when, how, and to what extent information about them can be transmitted to others. Security is defined as the protection of data against accidental or intentional disclosure to unauthorized persons or entities, or against unauthorized modification or destruction (Udo 2001). As mentioned above, while prior research has investigated the role of privacy concerns in determining the intention to or actual adoption of PETs, there is, as yet, no research focused on security concerns. However, due to the internet now being an integral part of our lives, security becomes the protection of everything we do in the online world, from purchasing goods and services, to browsing history; from remotely managing domestic appliances, to personal data storage; from preventing illegal access to our social networks, to protecting our bank accounts from criminal intrusion. In fact, it is no wonder that previous scholars focusing on technological aids for processing payments (e.g. Morosan and De Franco 2016) or online tax filing (e.g. Carter et al. 2011) used security related constructs as determinants of intention to use these technologies. Thus, in line with previous reasoning and with previous research findings, we expect that the higher the individual's security concerns, the higher the intention to adopt PETs. H2 is thus put forward as follows:

H2 Security concerns directly and positively influence users' intention to adopt PETs.

3.3 The mediation of UTAUT2

We have hypothesized the existence of a direct effect between, on the one hand, the constructs composing the UTAUT2, i.e. performance expectancy, effort expectancy, social influence, facilitating conditions, and hedonic motivation, and on the other hand, intention to adopt. We have also hypothesized a positive relationship between security concerns and intention to adopt PETs. Following an approach in line with previous contributions (e.g. Park et al. 2015; Jackson et al. 2013), we now also hypothesize a mediation effect of the considered UTAUT2 variables, in the relationship between security concerns and intention to adopt PETs. The increased consumers' awareness of security issues, conveyed through enhanced levels of their concerns, extends technological-utilitarian motives and additionally encompasses subjective and social considerations. This is confirmed by, among other things, the proliferation of PET-focused websites, online communities, dedicated forums, and more generally, by the increased media coverage these emerging technologies are gaining. Therefore, the assumption that the relationship between security concerns and users' intention to adopt PETs can be mediated by a comprehensive set of intrinsic-extrinsic as well as cognitive-affective drivers, such as those included in the UTAUT2, seems to be reasonable and logically supported (Venkatesh et al. 2012). Scholars have in fact found that constructs like the TAM's perceived usefulness and ease of use—which are substantially identical to UTAUT and UTAUT2's performance expectancy and effort expectancy—mediate the effects of security concerns (Müller-Seitz et al. 2009) or perceived security (O'Cass and Fenech 2003) on the use or intention to use mainstream Web technologies. Similarly, hedonic motivations have been found to positively mediate the effect between perceived security and adoption of online technologies, such as e-banking solutions (Salimon et al. 2017). Finally, considering that users also turn to social environments like online communities to better define their intrinsic concerns (i.e. for self-discovery purposes, see Dholakia et al. 2004), we further postulate that social influences mediate the effect of security concerns on the intention to adopt PETs. Therefore, we propose the third hypothesis:

H3 Performance expectancy (H3a), effort expectancy (H3b), social influence (H3c), facilitating conditions (H3d), and hedonic motivation (H3e) mediate the direct and positive relationship between security concerns and users' intention to adopt PETs.

3.4 Accounting for users' expertise

The moderating role of user expertise on users' intention or behavior has been theorized, included, and tested in multiple technology acceptance settings (Kim and Malhotra 2005; Venkatesh et al. 2003; Xu and Gupta 2009; Castañeda et al. 2007; Venkatesh et al. 2012). In the specific context of adopting communication anonymizers, accounting for users' expertise seems to be paramount, given that different users not only understand online anonymity differently, but also seek different strategies for obtaining it (Sardà et al. 2019; Shelton et al. 2015; Kang et al. 2013). Often, especially in computer-mediated communication, users can fall victim to a presumption of anonymity, i.e. they assume they are completely anonymous, even though their data is actually exposed. Different degrees of technical ability and familiarity with the technological context can play differential roles in the use of anonymity-granting technologies (Wallace 2008). Moreover, many non-experienced users lack the required awareness of the threats and the situations that require a security tool (Acquisti and Grossklags 2005). In other words, more experienced users are more likely than the less experienced to have the background and the skills set required to become acquainted with and develop the kind of concern that will assist them in perceiving the efficacy and performance of the technology. Thus, we hypothesize the following:

H4 The relationship between security concern and users' intention to adopt PETs is stronger for more experienced users than for less experienced users.

H5 The mediation effect of performance expectancy (H5a), effort expectancy (H5b), social influence (H5c), facilitating conditions (H5d), and hedonic motivation (H5e) between security concerns and users' intention to adopt PETs is stronger for more experienced users than for less experienced users.

All of the research hypotheses presented above are depicted in Fig. 1.

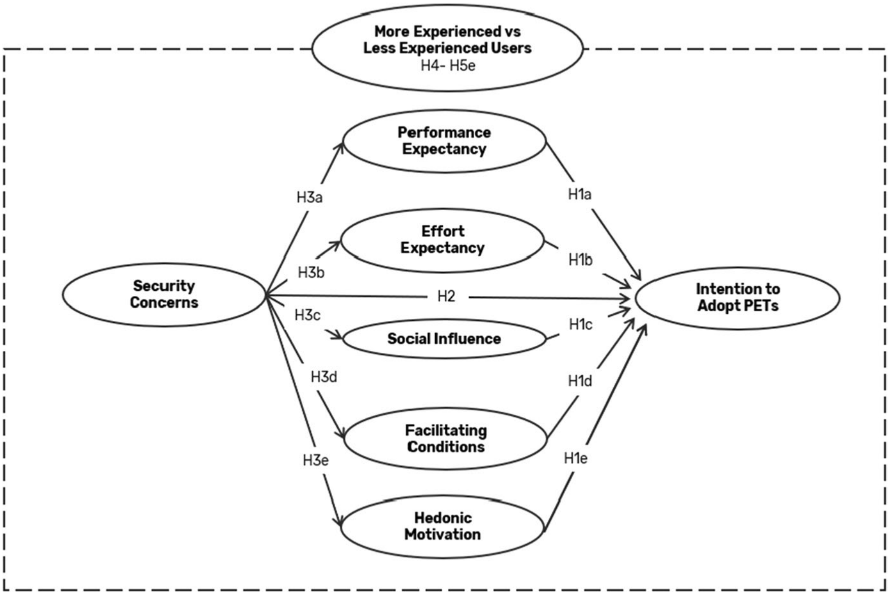

Fig. 1 Baseline model and tested hypotheses

4 Method

4.1 Data collection strategy

To collect the data, we focused on online communities in which discussions about PETs take place. Such online discussions take place on various websites that are established and managed either by technology vendors, or by users. Among these, Reddit (www.reddit.com) was chosen as the preferable setting for data collection. Due to its typical structure, i.e. divided in multiple interrelated subforums, Reddit allows the researcher to target specific interest groups (Shatz 2015) and to mitigate the recruited respondents' self-selection bias (Shatz 2016). Further, Reddit is basically a network of communities established, managed, and made active by users without any external party intervention. In this way, supposedly, the platforms become more lively, thus stimulating a higher sense of participation, commitment, and belonging compared to others that are similarly focused on the same issues, but established and managed by technology providers (Pedeliento et al. 2020). The questionnaire we administered was submitted to the communities listed in Table 2, which are all characterized by being closed, moderated, and guided by strict rules and codes of conduct. Any post must be submitted to a gatekeeper before it will be published. Posting surveys and questionnaires is usually banned, with only a few exceptions allowed after a thorough negotiation process with the subforum's moderators who review and suggest changes to the survey to make it compliant with the community standards. In our case, this process led to a shift from mainstream, data-tracing services like Google Form, which the community members perceive as intrusive, to more privacy and security friendly ones like Survey Monkey (surveymonkey.com) and Block Survey.io (blocksurvey.io). Thus, we used the latter two to collect the data. The moderators granted us access to the requisite communities; in addition to asking for precise details on the research purposes and the researchers' affiliation, and carefully checking the questionnaire's content, they explicitly endorsed the data collection, thus granting our data collection legitimacy among the community members. Conducting research about phenomena which can encompass stigmatized activities or hidden actors entails significant technical as well as ethical complications (Barratt and Maddox 2016). Gathering data which depicts internet users' intention to adopt anonymity-granting technologies means working with

Table 2 Reddit's PETs focused communities we used in data collection

Community	Members[a]	Description
r/security[b]	153,712	A friendly and professional place for discussing computer security
r/onions	208,306	The best parts of the anonymous internet
r/VPNTorrents	22,867	This is for the discussion of torrenting (and similar P2P protocols) using VPN type technology
r/VPN	89,662	References for understanding and building VPNs

[a] As on 5/6/2020

[b] Now closed down and moved to r/cybersecurity

participants who are likely to be concerned about the security of their online identities. As one could expect, these participants' general mistrust and unwillingness to provide and share any kind of information relatable to the self makes data collection difficult. To illustrate this, despite having followed and guaranteed a research protocol aimed at securing the respondents' anonymity throughout the entire data collection phase, we still encountered some evocative manifestations of suspicion and resistance from target respondents, in comments anonymous users posted beneath our survey, such as "*I like to protect my privacy by not filling out online surveys*" (User_name1), or "*I think the number of people who refuse to fill out this survey would actually make for a useful data point in this study*" (User_name2).

4.2 Survey instrument

The questionnaire was structured in two parts. The first part asked for the respondents' demographic information, such as gender, age, place of residence, profession, and education. These questions asked participants to respond voluntarily, showing consideration and respect for the respondents' sensitivity to anonymity.

The second part listed a set of observed variables to measure the constructs composing the theoretical framework tested. We drew the variables of the UTAUT2 from Venkatesh et al. (2012) and adapted them to the specific context of PETs. Due to the lack of sufficiently reliable and valid measurement scales in the extant literature, we derived items measuring the latent variable of security concern from the multidimensional Addae et al.'s (2017) Personal Data Attitude (PDA) scale. The usage of a single dimension of the overall measurement scale allowed us to compose a measure of security that minimize conceptual and operational overlap with similar measures of privacy concerns. We measured all the items on a 7-point Likert scale, ranging from 1 (totally disagree) to 7 (totally agree). However, for measuring users' expertise with PETs we used a self-reported measure of expertise allowing them to choose from a set of three different options: (1) high level of expertise with PETs (more than 12 months of experience using PETs); (2) moderate level of expertise with PETs (from 6 to 12 months of experience using PETs); (3) low level of expertise with PETs (less than 6 months of experience with PETs).

5 Results

5.1 Sample of respondents

We posted the survey to Reddit communities in two waves, to account for the fact that the highest interaction in the subforums typically occurs during the first 24 h after the initial posting (Moyer et al. 2015; Shatz 2015). The first wave resulted in 118 responses. After 14 days, we sent a reminder, resulting in additional 124 additional responses. Although compared to the actual size of the communities the response rate is low (<1%), it is in line with previous research focused on PET adoption (e.g. Harborth and Pape 2019) and with previous studies conducted on

Reddit-based communities (Shatz 2016). Overall, 221 respondents completed the questionnaire. Of these, 18 were discarded because respondents disclosed they have never used anonymizers before, and another five responses were excluded due incomplete data. The final sample of responses, hence, was composed of 198 questionnaires. To avoid non-response biases, we used the technique advocated by Armstrong and Overton (1977), comparing the subject responses received from different communities and different waves. No significant differences were found regarding independent variables or criterion variables.

Table 3 shows the socio-demographic characteristics of our sample: respondents' average age was 29, while 104 (53%) were male, 38 (19%) female, and 56 (28%) did not declare their gender. We compared this socio-demographic data to that of the population from which it was drawn (GlobalWebIndex 2018b, c) as well as to other samples used in previous research (Spiekermann 2005), and judged our sample to be representative. Notably, the number of respondents who opted not to give demographic information, is relatively high. As previous studies suggest, the investigated population's significant concern about privacy and security can be considered the main reason why respondents were reluctant to share this information (Harborth et al. 2020). Finally, regarding the level of expertise with anonymizers concerned in the study, the results revealed that the sample of respondents is almost evenly split into two proportionate groups of users. The first declared themselves to have a high level of PET expertise (48% of the sample), named the more experienced users, and the second self-assessed their degree of PET expertise as moderate account or low (52% of the sample), named less experienced users).

5.2 Measurement model

To test the hypotheses, we first conducted an exploratory factor analysis (EFA) using the Maximum likelihood procedure with the Direct Oblimin rotation method,

Table 3 Description of the sample

	Freq.	Perc.
N = 198 average age 29		
Gender		
Female	38	19
Male	104	53
Not declared	56	28
Education		
Ph.D.	10	7
Master degree	47	32
Bachelor degree	43	29
High-school diploma	47	32
Expertise		
More experienced users	94	48
Less experienced users	104	52

and we successively tested the structural equation model analysis (Steenkamp and Baumgartner 1998) with AMOS 23.0 program.

Accordingly, we conducted an EFA to test the convergent and discriminant validity of the adapted conceptual model (Tabachnick and Fidell 2007). Items with low communality scores ($< .4$) were discarded as they represent problematic items (Field 2013). We then reran a further EFA analysis which produced a simple solution comprising six factors. Most of the items loaded on separate factors with factor loadings exceeding the .4 threshold (Field 2013), with all cross-loadings on other factors being insignificant, so that we conclude there are no convergent and discriminant validity issues in this EFA solution (Fornell and Larcker 1981). This test led us to discard one item from the construct performance expectancy, three items from intention to use PETs, and the full construct of facilitating conditions.

Successively, we ran a CFA to validate the measures and to define the relations between observed and latent variables. We established a six-construct measurement model with the remaining 19 observed variables. The measurement model's goodness of fit statistics revealed a good fit. The ratio between the Chi square ($\chi^2 = 201.899$; $p < .000$) and degrees of freedom ($df = 137$) is below 2 (Tabachnick and Fidell 2007) and all other relevant fit indexes overcome the recommended thresholds: RMSEA = .049; CFI = .967; NNFI = .959. The constructs showed excellent internal consistency: Cronbach's alphas ranged from a minimum of .76 to a maximum of .88. Moreover, the composite reliability (CR) and average variance extracted (AVE) of each construct were above the recommended threshold levels of .6 and .5 respectively (Bagozzi and Yi 1988). The model met the requirements for convergent validity, with each item loading significantly and substantially (above .5) on the expected latent construct (Table 4).

Moreover, in order to reduce the risk of common methods bias for data, we employed Harman's single-factor test (Podsakoff et al. 2003). We estimated a CFA to compare our model to a constrained single-factor model. In case of common method variance, the single latent factor would account for all of the variables. The single-factor fit showed no evidence of common method bias, as it exhibited $\chi^2 = 1066.59$ and df = 152. Thus, the measurement model demonstrated significantly improved fit ($p < .001$).

Finally, following Fornell and Larcker (1981), we assessed the discriminant validity of each construct, by comparing the AVE values with the squared correlations for all pairs of latent variables. As the highest squared correlation is .525 and the lowest related AVE is .679, all pairs of constructs met this condition (Table 5).

5.3 Structural model

The structural model showed an excellent level of fit: $\chi^2 = 201.899$; df = 137; $p < .000$; RMSEA = .049; NNFI = .959; CFI = .967. The test of the direct relationship between UTAUT2 constructs included in the model and the *users' intention to adopt PETs* was supported. In particular, the results show that *performance expectancy* (H1a), *effort expectancy* (H1b), *social influence* (H1c), and *hedonic motivation* (H1e) are all directly and positively related to *users' intention to adopt PETs*. We did

Table 4 Overall CFA for the measurement model

Constructs and measurement items	Std. loadings (t value)	Mean	SD	CA	CR	AVE
Users' intention to adopt PETs				*.807*	*.850*	*.740*
Using an anonymizer is something I would like to do	.921 (std.)	4.80	1.84			
I will try to use an anonymizer in my daily life	.795 (12.62)	4.33	1.98			
Performance expectancy				*.911*	*.886*	*.723*
I think that anonymizers allow me to do things faster	.785 (std.)	3.15	1.58			
I think anonymizers improve my performance	.898 (13.65)	3.24	1.65			
Anonymizers can improve my productivity	.863 (13.14)	3.15	1.56			
Effort expectancy				*.905*	*.888*	*.666*
Learning how to use anonymizers is easy for me	.855 (std.)	5.16	1.75			
I find anonymizers easy to use	.803 (13.06)	5.10	1.58			
Using anonymizers is a clear and understandable activity	.834 (13.75)	4.76	1.70			
It is easy to become skillful in using anonymizers	.770 (12.33)	4.93	1.54			
Social influence				*.911*	*.762*	*.502*
People who are important to me agree that I should use anonymizers	.721 (std.)	3.16	1.745			
People whose opinions I value think that I should use anonymizers	.794 (8.60)	3.20	1.717			
People I respect use anonymizers	.635 (7.95)	3.30	1.636			
Hedonic motivation				*.830*	*.864*	*.679*
Using anonymizers is fun	.858 (std.)	3.64	1.64			
Using anonymizers is pleasant	.786 (12.55)	4.17	1.61			
Using anonymizers is entertaining	.827 (13.39)	3.49	1.60			
Security concern				*.858*	*.811*	*.519*
I am concerned that certain information is lost due to the lack of adequate security measures	.817 (std.)	5.16	1. 454			
I believe that stricter security measures are needed to ensure the correctness of particularly personal information	.635 (8.50)	5.87	1.410			

Table 4 (continued)

Constructs and measurement items	Std. loadings (t value)	Mean	SD	CA	CR	AVE
I am concerned that incorrect information is linked to my identity due to security breaches	.704 (9.44)	5.32	1.559			
I am concerned that the databases containing my personal information are not protected from unauthorized access	.714 (9.56)	5.51	1.509			

[a] The construct of facilitating conditions was deleted due to low statistical fit

Note: Items of the constructs adapted from the mentioned authors and amended and fitted into our contexta and the construct of facilitating conditions was deleted due to low statistical fit

Table 5 Correlations among constructs

Constructs	(1)	(2)	(3)	(4)	(5)	(6)
(1) Users' intention to adopt PETs	1					
(2) Effort expectancy	.317	1				
(3) Performance expectancy	.681	.234	1			
(4) Hedonic motivation	.687	.330	.725	1		
(5) Social influence	.616	.216	.474	.453	1	
(6) Security concern	.510	.043	.234	.387	.449	1

not test for the hypothesized relationship between *facilitating conditions* and *users' intention to adopt PETs* (H1d), nor for its mediation effects (H3d and H5d) due to the exclusion of the construct *facilitating conditions* from the analysis. The results of the structural model (see Table 6) also provided support for H2, i.e. that *security concerns* and *users' intention to adopt PETs* are directly and positively related (ß = .18; p < .01). Moreover, we found that *security concern*s explain *social influence* (ß = .45; p < .00), *hedonic motivation* (ß = .39; p < .00), and *performance expectancy* (ß = .37; p < .00), but not *effort expectancy*. Finally, to provide a test of H3, i.e. that *performance expectancy* (H3a), *effort expectancy* (H3b), *social influence* (H3c), and *hedonic motivation* (H3e) mediate the direct and positive relationship between *security concerns* and *users' intention to adopt PETs*, we followed a procedure of controlling for covariances among mediators to achieve better and more reliable estimates for specific indirect effects. To test for indirect effects, we decided not to use the Sobel Test because it assumes a symmetric distribution of the indirect effect and therefore would lead to biased results. Rather, we applied MacKinnon's (2008) procedure which consists in computing a 95% asymmetric confidence interval for each specific indirect effect using PRODCLIN software (MacKinnon et al. 2007). As Table 7 shows, *social influence* and *hedonic motivation* mediate the relationship between *security concern* and *users' intention to adopt PETs*. Hence, H3c, and H3e are supported. The data, however, did not support the hypothesized mediation of

Table 6 Standardized direct effects

	β	SE
Security concerns → Users' intention to adopt PETs	.181**	.097
Security concerns → Social influence	.449*	.091
Security concerns → Hedonic motivation	.387*	.101
Security concerns → Performance expectancy	.377*	.086
Security concerns → Effort expectancy	n.s.	n.s.
Social influence → Users' intention to adopt PETs	.275*	.091
Hedonic motivation → Users' intention to adopt PETs	.258**	.113
Performance expectancy → Users' intention to adopt PETs	.266**	.128
Effort expectancy → Users' intention to adopt PETs	.127***	.169

*p < 0.00; **p < 0.01;***p < 0.05

Table 7 Standardized indirect and total effects of security concern on intention to adopt PETs

Specific indirect effect	Total effect	Indirect effect	95% Asymmetric confidence interval		sig. (p <.05)
			Lower bound	Upper bound	
Security concerns → Social influence → Users' intention to adopt PETs	.457*	.510*	.032	.257	p <.05
Security concerns → Hedonic motivation → Users' intention to adopt PETs			.012	.242	p <.05
Security concerns → performance expectancy → users' intention to adopt PETs			.000	.244	n.s
Security concerns → effort expectancy → users' intention to adopt PETs			− .017	.039	n.s.

*p <.00

performance expectancy and *effort expectancy*. Hence, we rejected H3a and H3b which gives only partial acceptance of H3.

5.4 Multigroup analysis

Besides testing for direct and indirect effects of the theoretical model specified in this research, we also tested additional hypotheses based on the users' level of expertise. In detail, we found that the relationship between security concern and users' intention to adopt PETs is stronger for more experienced users than for less experienced users (H4), and that the mediation effect of performance expectancy (H5a), effort expectancy (H5b), social influence (H5c) and hedonic motivation (H5e) between security concerns and users' intention to adopt PETs is stronger for less experienced users than for more experienced users. The structural equation model made it possible to control for the covariance between the mediator and thus to obtain more reliable estimates for specific indirect effects. We tested indirect effects applying MacKinnon's (2008) procedure by using PRODCLIN software (MacKinnon et al. 2007).

The measurement model estimated for the two groups independently (more and less experienced) demonstrated a good fit with the data, both for the more experienced ($\chi^2=221.261$; $p=.00$ df = 137; RMSEA = .081; CFI = .904; NNFI = .880), and for the less experienced ($\chi^2=167.616$; $p=.03$; df = 137; RMSEA = .047; CFI = .971; NNFI = .964). To test whether the two samples show the same factor pattern, we ran the configural invariance test, that showed a good fit ($\chi^2=338.951$; $p=.00$ df = 274; RMSEA = .046; CFI = .941; NNFI = .926). In order to verify that the interpretation of item measurement between more and less experienced users is the same, we tested the metric invariance. In this case, the results also showed a good fit ($\chi^2=410.258$; $p=.00$; df = 287; RMSEA = .047; CFI = .936; NNFI = .926) and the univariate χ^2 incremental value reveals that the probability value is higher than .05.

Finally, we conducted a test of structural invariance to verify that a structural model specified in one sample (e.g. more experienced users), replicates in a second independent sample from the same population (e.g. less experienced users). In particular, we started by testing H4, i.e. that the relationship between *security concern* and *users' intention to adopt PETs* is stronger for more experienced users than for less experienced users. The results show that this relationship is significant only for more experienced users (ß = .43; $p < .00$), while it is not statistically significant for the group of less experienced users (ß = .04; $p > .05$). We then proceeded to test the mediation effect of the retained UTAUT2 variables, i.e. *performance expectancy* (H5a), *effort expectancy* (H5b), *social influence* (H5c), and *hedonic motivation* (H5e) in the relationship between *security concerns* and *users' intention to adopt PETs*. The results show that while the relation between *security concerns* and *users' intention to adopt PETs* is significant and non-mediated for more experienced users, this relationship, contrastively, is fully mediated by *social influence* and *hedonic motivations* for the less experienced users. The mediation effect of the other variables included in the model, i.e. performance and efforts expectancy, are non-significant, so that we find only partial support for H5 (see Table 8).

6 Discussion

This study expands the still nascent user-focused research aimed at understanding what may drive and what may obstacle end-user's acceptance and subsequent adoption of more popular PETs like communication anonymizers. In particular, it has been designed to address an overlooked phenomenon in the PET-related domain, that is related to how users' security concerns affect their intention to adopt PETs. The results show that the predictive power of the UTAUT2 model (Venkatesh et al. 2012) holds even when the intention to use PETs is of concern. All of the constructs we retained, namely *performance expectancy*, *effort expectancy*, *social influence,* and *hedonic motivations*, were found to be significantly and positively related to *users' intention to adopt PETs*. Even though previous research has already proven that technical considerations are pivotal in determining the acceptance of these technologies (Harborth et al. 2020), our findings provide the very first empirical evidence that, at least at the intentional stage, social and hedonic aspects are equally taken into account by PET adopters. Recall that, differently to the originally specified model, we discarded the construct *facilitating conditions* (which is a constitutive part of both the UTAUT and the UTAUT2), as it failed the EFA. Indeed, this construct, with its underlying meaning is operationalized in such a way that it overlaps with both the UTAUT's *effort expectancy* and the TAM's *ease of use* (Venkatesh et al. 2003), and has for this reason similarly been discarded in other empirical research focused on similar technological contexts (Shawn and Sergueeva 2019). A possible explanation for the statistical inconsistency of the *facilitating conditions* construct in our results could lie in the fact that the construct includes the extent and type of support provided to aid technology use, and the fact that despite being around for a while, this kind of support has only limitedly been rolled out (especially compared to other technologies). In contrast, our results reveal that *security concerns* do prompt users' intentions to adopt PETs for both more and less experienced users, which confirms the motivational role of the "personal threat model," making it one of the key reasons for users' turning to anonymous browsing (Kang et al. 2013). As the frequency with which episodes of online security violation rises, individuals' concerns about the possibility that third parties will encroach on and manipulate their personal data increases. Thus, a growing share of internet users take precautions. The general finding, however, that these technologies should be perceived as useful, easy to use, as well as socially accepted and enjoyable by the end-user is not very informative *per se* (Shawn and Sergueeva 2019). Therefore, we sought a theoretical explanation as to why constructs composing the UTAUT2 could be considered as mediators of the relationship between *security concerns* and *intention to adopt PETs*. The analysis revealed that while two of the UTAUT's core constructs, i.e. *performance expectancy* and *effort expectancy*, do not play any significant mediating role in this relationship, the others, i.e. *hedonic*

Table 8 Standardized indirect and total effects of *security concern* on *intention to adopt PETs* for more experienced and less experienced respondents

Specific indirect effect	Total effect	Indirect effect	95% Asymmetric confidence interval		sig. ($p < .05$)
			Lower bound	Upper bound	
More experienced users					
Security concerns → social influence → users' intention to adopt PETs	.691*	.188*	− .027	.168	n.s.
Security concerns → Hedonic motivation → Users' intention to adopt PETs			− .038	.246	n.s.
Security concerns → performance expectancy → users' intention to adopt PETs			− .023	.255	n.s.
Security concerns → effort expectancy → users' intention to adopt PETs			− .011	.051	n.s.
Less experienced users					
Security concerns → social influence → users' intention to adopt PETs			.043	.544	$p < .05$
Security concerns → Hedonic motivation → Users' intention to adopt PETs			.196	.205	$p < .05$
Security concerns → performance expectancy → Users' intention to adopt PETs	.419*	.426*	− .004	.357	n.s.
Security concerns → effort expectancy → users' intention to adopt PETs			− .058	.023	n.s.

motivation and *social influence*, do mediate the relationship. The perceived enjoyment, pleasure, or fun derived from using these applications (condensed in the *hedonic motivations* construct) together with social pressure that relatives, colleagues, or peers exert (described by the latent variable of *social influence*), significantly influence the individual's choice to adopt the technology. Also, they have the power to amplify the primary reason for users turning to PETs, i.e. to address their security concerns. These findings support the view that online anonymity-granting technologies have a function and associated meanings that go beyond their technical/utilitarian features to additionally encompass others that relate to the social as well as the individual sphere (Wallace 2008). Nevertheless, we identified important differences between the groups. The results of the multi-group analysis of more and less experienced users clearly show that the effect of *security concerns* on the *users' intention to adopt PETs* is tightly connected to the relative degree of users' technological expertise. In detail, *security concerns* are significant and direct drivers of *users' intention to adopt PETs*, that are limited to the cluster of more experienced users. For this group of respondents, the results did not support the hypothesized mediation of the UTAUT2 constructs in the relationship between *security concerns* and *intention to adopt PETs*. Therefore, based on the results, we can infer that for more experienced users, the will to achieve a solution to their *security concerns* is a sufficient condition prompting their decision to use online anonymizers. This category of users, in fact, is likely to possess the technological knowledge and technical expertise required to master these technologies, making other conditions, especially those related to hedonic and social aspects related to technology use, less important. Using online anonymizers is not easy at all, and their adoption requires a higher level of technical knowledge than regular internet users have; they can make online navigation slower, more challenging, and less spontaneous. Differently stated, *security concerns* have such an important role in experienced users' needs hierarchy that *per se* they justify turning to these technologies, regardless of whether they meet their performance and effort expectations, and no matter whether they are enjoyable or socially acceptable.

In the case of less experienced users, the relation between *security concerns* and *intention to adopt PETs* was found to be fully mediated only by *social influence* and *hedonic motivations*. Thus, for those less experienced, *security concerns* alone are not sufficient to explain their intention to adopt. These users need support to understand the risks and implications of a potential misuse of their personal data and of the tools they can apply to achieve higher levels of security. Differently stated, the likelihood of less experienced users adopting a PET is connected to the technology's ability to satisfy their hedonic needs, as well as to the social acceptance and legitimacy these technologies have among others.

Owing to the importance of social forces in fostering users' willingness to adopt PETs, it is little wonder that several online communities and discussion forums have recently emerged. The aim of these communities is not limited to familiarizing people with how to use technologies, but also—and perhaps foremost—to evangelize others regarding the importance of protecting their online lives and their online security. These communities, in fact, often tend to focus on security concerns by emphasizing the ideology that underpins online anonymity rather than on the technical means users' can leverage to achieve higher levels of online privacy and security. This, we contend, is perhaps the main reason why less experienced users rate social influences as more relevant than more experienced ones do.

6.1 Practical implications

This article's findings have several managerial implications addressed at two different target audiences. The first are firms that have an online presence, i.e. that have entirely online business models and/or that conduct a part of their business operations online. The second are firms whose business is to develop, distribute, and sell PETs. For the former, our results suggest that they should pay increasing attention to issues concerning the felt online security of their prospective and actual consumers. The more the internet's penetration in people's lives increases, the more security issues will assume importance. Security hence will play an increasingly important role in driving consumers' purchasing choices and—for this reason—is expected to affect new product and new business development, as well as business communication and advertising. The use of anonymizers in particular, can seriously endanger the long-term survival of those data-driven companies that need to collect and analyze a large number of consumers' behavioral and traffic data to take decisions and to predict future scenarios. Companies like Google, Amazon, Facebook, and other tech-giants could sustain serious damage if internet users were to turn to online anonymizers *en masse,* as they would necessarily have to find new ways of monetizing internet traffic. Problems could also emerge for companies selling their goods and services via online channels if they are unable to assure the highest levels of security to prevent cyber-attacks and cyber fraud that could discourage consumers from purchasing online. Again, the more online security concerns attract general attention, the higher the likelihood that consumers will place security at the top of their priorities list. Besides continuing to develop and adopt technologies and systems aimed at increasing online security, it is important that managers develop a strategic communication focused on security issues. This can be shaped to reassure consumers of the security of their online data, information, and identities, and could even represent a key selling point to differentiate their own offering vis-à-vis that of competitors.

Regarding PET developers, the findings underline the importance of evaluating both intrinsic and extrinsic motivations as main determinants of the intention to adopt online anonymizers. We thus recommend that developers seriously consider the effects of hedonic motivation and social influence in prompting users to adopt these technologies, while putting less emphasis on technology-specific issues that will possibly be taken for granted once the online anonymizers have increased their penetration and become widely diffused. On a tactical level, we suggest that PET developers attend more to the level of engagement that users can experience by using PETs, for example by underlining the fun and entertainment installing, using, and updating an anonymizer offers. Also, they should play a more active role in influencing the social debate on online security to emphasize how useful PETs can be. Differently stated, we suggest these companies should act as ideological proselytizers (Holt 2006) that stand beside communities and social movements committed to making the internet a more secure and less surveilled place. This could be especially effective for PET developers targeting less experienced consumers who are more likely to be convinced to use anonymizers if they are perceived as entertaining, as well as socially accepted and endorsed. To these aims, developing new communities and movements or supporting existing ones, regardless of whether they are online or off-line, with a focus on online security, can be an effective way for managers to shape the social debate on these issues, thereby also serving their own profit and interest.

6.2 Limitations and further research

The results and the implications of this article should be read with certain limitations in mind. The first limitation relates to the sample that we used in the study. We collected the data from a community of users that have a fair level of expertise on PETs. Therefore, we need further to test the validity of our proposed empirical model on a sample of respondents characterized by very low technological readiness and a lower level of familiarity with online anonymizers than our sample. This could be of great importance if PET is to achieve higher rates of penetration and mass-market diffusion, as shedding more light on ‘regular’ users would attend to the ones that need to be engaged and convinced of the value anonymizing can bring. The second limitation pertains to the methodology we used in our study. We relied on quantitative methodologies because they allow for collecting a large amount of data with relatively low effort; however, the using a qualitative methodology could be fruitful to complement our findings and delve deeper into some issues that we still do not fully understand. For example, although our findings show that social influence plays a major role in users’ intention to adopt PETs, we still know very little about what these social forces are and how they shape the environment that most likely fosters and eventually boosts adoption. A third limitation relates to the number of variables and of mediating variables we used. Despite the UTAUT2 being well suited to provide solid insight on what motivates users’ adoption or intention to adopt technologies, it remains limited to a finite number of variables and does not exclude the possibility that other factors can influence intention. Finally, the substantial lack of moderating variables in the model we tested should be recognized as a limiting concern. The UTAUT2 model generally implies the use of moderators such as age, gender, and expertise; nevertheless, while we took expertise into account, we did not include age and gender because managers of the communities we targeted for data collection did not allow us to request this kind of information as it was deemed to be too intrusive in a user community highly concerned about privacy and security. Thus, we cannot indicate whether age and gender affect the hypotheses we tested. In addition, it has to be noted that the moderating variable of expertise used was a self-reported measure. Despite the characteristics of the respondents included in the sample, i.e. people that share a common interest in PETs usage, allow minimizing the risks implicit in the usage of self-reported measures of expertise, biases that may stem from the usage of such measures (e.g. social desirability bias, Crowne and Marlowe 1960) cannot be neglected and require to be outlined especially for the sake of results' generalizability.

7 Conclusion

Internet and web-based technologies' increased role in our lives is attracting a great deal of attention, especially regarding the security and privacy related risks implied in using the internet for communication, purchasing, and work-related reasons. This explains the multiple technologies that consumers currently can use to achieve higher levels of online anonymity and greater online security. These technologies fall under the umbrella label of PETs—privacy enhancing technologies—that, despite gaining momentum, according to the current literature are still rarely investigated and poorly understood.

This paper confirms that extant research tends to focus on privacy and neglects issues related to online security. With the aim to fill existing gaps in the emerging literature, our research was designed to gain understanding of how users' security concerns affect their intention to adopt PETs. To achieve this aim, we developed a theoretical framework based on the UTAUT2, tested a set of underlying hypotheses, and compared the suggested model's predictive validity by also accounting for users' expertise. The results we report suggest that despite UTAUT's variables predicting intention to adopt PETs, their most important role is one of mediating the relationship between security concerns and intention to adopt PETs, with special reference to the group of users that have lower levels of expertise. However, due to the wide global diffusion of PETs, the need for further investigation of motives prompting users to adopt such PETs remains.

Funding No funding to declare.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Acquisti, A. (2004). Privacy and security of personal information: Economic incentive and technological solutions. In J. Camp & R. Lewis (Eds.), *The economics of information security* (pp. 1–9). Dordrecht: Kluwer.

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*(1), 26–33.

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information and Computer Security, 25*(5), 560–579.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50,* 179–211.

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management, 37*(3), 99–110.

AlSabah, M., & Goldberg, I. (2016). Performance and security improvements for tor: A survey. *ACM Computing Surveys (CSUR), 49*(2), 1–36.

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). *The consumer-data opportunity and the privacy imperative*. McKinsey and Company. Retrieved July 16, 2020 from, https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research, 14*(3), 396–402.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74–94.

Bandura, A., Freeman, W. H., & Lightsey, R. (1999). Self-efficacy: The exercise of control. *Journal of Cognitive Psychotherapy, 13*(2), 158–166.

Barlett, C. P., & Gentile, D. A. (2012). Attacking others online: The formation of cyberbullying in late adolescence. *Psychology of Popular Media Culture, 1*(2), 123.

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research, 16*(6), 701–719.

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.

Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenberg, K., & Stamatiou, Y. (2014). User acceptance of privacy-ABCs: An exploratory study. In *International conference on human aspects of information security, privacy, and trust* (pp. 375–386), Springer, Cham.

Benenson, Z., Girard, A. & Krontiris, I. (2015). User acceptance factors for anonymous credentials: An empirical investigation. In *14th Annual Workshop on the Economics of Information Security (WEIS),* (pp. 1–33).

Borking, J. J. (2011). Why adopting privacy enhancing technologies (PETs) takes so much time. In S. Gutwirth, Y. Poullet, P. De Hert, & R. Leenes (Eds.), *Computers, privacy and data protection: An element of choice*. Dordrecht: Springer.

Borking, J. J., & Raab, C. (2001). Laws, PETs and other technologies for privacy protection. *Journal of Information, Law and Technology, 1,* 1–14.

Brecht, F., Fabian, B., Kunz, S., & Mueller, S. (2011). Are you willing to wait longer for internet privacy? *ECIS Proceedings, 2011,* 214.

Brecht, F., Fabian, B., Kunz, S., & Müller, S. (2012). Communication anonymizers: Personality, internet privacy literacy and their influence on technology acceptance. *ECIS Proceedings, 2012,* 214.

Carter, L., Shaupp, L. C., Hobbs, J., & Campbell, R. (2011). The role of security and trust in the adoption of online tax filing. *Transforming Government: People, Process and Policy, 5,* 303–318.

Castañeda, J. A., Muñoz-Leiva, F., & Luque, T. (2007). Web acceptance model (WAM): Moderating effects of user experience. *Information & Management, 44*(4), 384–396.

Caulfield, T., Ioannidis, C., & Pym, D. (2016). On the adoption of privacy-enhancing technologies. In Q. Zhu, T. Alpcan, E. Panaousis, M. Tambe, & W. Casey (Eds.), *Decision and game theory for security. GameSec. 2016 Lecture notes in computer science* (Vol. 9996). Cham: Springer.

Chellappa, R. K. (2008). *Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security*, Unpublished paper, Emory University, Atlanta, USA.

Clark, J., Van Oorschot, P. C., & Adams, C. (2007). Usability of anonymous web browsing: An examination of tor interfaces and deployability. In *Proceedings of the 3rd symposium on usable privacy and security* (pp. 41–51).

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology, 34*(1), 59–80.

Crowne, D. P., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology, 24,* 349–354.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–342.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. Doctoral dissertation, Massachusetts Institute of Technology.

Dholakia, U. M., Bagozzi, R. P., & Pearo, L. K. (2004). A social influence model of consumer participation in network-and small-group-based virtual communities. *International Journal of Research in Marketing, 21*(3), 241–263.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

European Union Agency for Network and Information Security (ENISA). (2016). *PETs controls matrix. A systematic approach for assessing online and mobile privacy tools. Final Report, December 2016*. Retrieved July 16, 2020 from, https://www.enisa.europa.eu/publications/pets-controls-matrix/pets-controls-matrix-a-systematic-approach-for-assessing-online-and-mobile-privacy-tools.

Fabian, B., Goertz, F., Kunz, S., Müller, S. and Nitzsche, M. (2010). Privately waiting—A usability analysis of the tor anonymity network. In *Proceedings 16th Americas conference on information systems (AMCIS 2010), selected papers* (Vol. 58). Springer LNBIP.

Feigenbaum, J., Freedman, M., Sander, T., & Shostack, A. (2002). Economic barriers to the deployment of existing privacy technology. In *Proceedings of the Workshop on Economics and Information Security, Berkley, CA*.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Thousand Oaks: Sage.

Fishbein, M. (1979). A theory of reasoned action: Some applications and implications. *Nebraska Symposium on Motivation, 27,* 65–116.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Fritsch, L. (2007). *State of the art of privacy-enhancing technology (PET)—Deliverable D2.1 of the PETweb project*; NR Report 1013, Norsk Regnesentral, ISBN 978-82-53-90523-5. Retrieved July 16, 2020, from, https://www.nr.no/publarchive?query=4589.

Galletta, D. F., Henry, R., McCoy, S., & Polak, P. (2004). Web site delays: How tolerant are users? *Journal of the AIS, 5*(1), 1–28.

Galperin, E. (2011). *Nymwars (in review)*. Electronic Frontier Foundation. Retrieved July 16, 2020 from, https://www.eff.org/it/deeplinks/2011/12/2011-review-nymwars.

Gan, M. F., Chua, H. N., & Wong, S. F. (2019). Privacy enhancing technologies implementation: An investigation of its impact on work processes and employee perception. *Telematics and Informatics, 38,* 13–29.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media and Society, 18*(7), 1219–1235.

Global Market Insights. (2020). *Global research report, VPN market size and share 2020–2026*. Retrieved July 16, 2020, from, https://www.gminsights.com/industry-analysis/virtual-private-network-vpn-market.

GlobalWebIndex. (2018a). *Share of internet users worldwide who have used a VPN in the past month as of 1st quarter 2018, by region* [Graph]. In Statista. Retrieved July 16, 2020, from, https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/.

GlobalWebIndex. (2018b). *Share of internet users worldwide who have used a VPN in the past month as of 1st quarter 2018, by age group* [Graph]. In Statista. Retrieved July 16, 2020, from, https://www.statista.com/statistics/301212/vpn-proxy-usage-age/.

GlobalWebIndex. (2018c). *Share of internet users worldwide who have used a VPN in the past month as of 1st quarter 2018, by gender* [Graph]. In Statista. Retrieved July 16, 2020, from, https://www.statista.com/statistics/301208/vpn-proxy-usage-gender/.

Ha, S., & Stoel, L. (2009). Consumer e-shopping acceptance: Antecedents in a technology acceptance model. *Journal of Business Research, 62*(5), 565–571.

Harborth, D., & Pape, S. (2018). *JonDonym users' information privacy concerns*. In L. Janczewski & M. Kutyłowski (Eds.), *ICT Systems Security and Privacy Protection. SEC 2018. IFIP Advances in Information and Communication Technology* (Vol. 529, pp. 170–184). Poznan, Poland: Springer, Cham.

Harborth, D., & Pape, S. (2019). How privacy concerns and trust and risk beliefs influence users' intentions to use privacy-enhancing technologies—The case of Tor. In *Hawaii international conference on system sciences (HICSS) proceedings* (pp. 4851–4860). Hawaii, US.

Harborth, D., Pape, S., & Rannenberg, K. (2020). Explaining the technology use behavior of privacy-enhancing technologies: The case of Tor and JonDonym. *Proceedings on Privacy Enhancing Technologies, 2020*(2), 111–128.

Herrero, Á., & San Martín, H. (2017). Explaining the adoption of social networks sites for sharing user-generated content: A revision of the UTAUT2. *Computers in Human Behavior, 71,* 209–217.

Heurix, J., Zimmermann, P., Neubauer, T., & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers and Security, 53,* 1–17.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketspace: Implications for the commercial uses of anonymity on the web. *The Information Society: An International Journal, 15*(2), 129–139.

Holt, D. B. (2006). Jack Daniel's America: Iconic brands as ideological parasites and proselytizers. *Journal of Consumer Culture, 6*(3), 355–377.

Identity Theft Resource Center. (2020). *Annual number of data breaches and exposed records in the United States from 2005 to 2019 (in millions)* [Graph]. In Statista. Retrieved July 16, 2020 from, https://www-statista-com.ezproxy.unibg.it/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

Jackson, J. D., Yi, M. Y., & Park, J. S. (2013). An empirical test of three mediation models for the relationship between personal innovativeness and user acceptance of technology. *Information & Management, 50*(4), 154–161.

Jardine, E. (2016). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media and Society, 20*(2), 435–452.

Kaaniche, N., Laurent, M., & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications, 171,* 102807.

Kang, R., Brown, S., & Kiesler, S. (2013). Why do people seek anonymity on the internet? Informing policy and design. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 2657–2666).

Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., & Vallina-Rodriguez, N. (2018). An empirical analysis of the commercial vpn ecosystem. *Proceedings of the Internet Measurement Conference, 2018,* 443–456.

Kim, S. S., & Malhotra, N. K. (2005). A longitudinal model of continued is use: An integrative view of four mechanisms underlying post-adoption phenomena. *Management Science, 51*(5), 741–755.

Krontiris, I., Benenson, Z., Girard, A., Sabouri, A., Rannenberg, K., & Schoo, P. (2015). Privacy-ABCs as a case for studying the adoption of PETs by users and service providers. In *Annual privacy forum* (pp. 104–123). Springer, Cham

Larsson, S., Svensson, M., & de Kaminski, M. (2012). Online piracy, anonymity and social change: Innovation through deviance. *Convergence: The International Journal of Research into New Media Technologies, 19*(1), 95–114.

Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., & Wagner, D. (2017). A usability evaluation of Tor launcher. *Proceedings on Privacy Enhancing Technologies, 3,* 90–109.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*(3), 191–204.

Lin, C. A., & Kim, T. (2016). Predicting user response to sponsored advertising on social media via the technology acceptance model. *Computers in Human Behavior, 64,* 710–718.

MacKinnon, D. P. (2008). *Introduction to statistical mediation analysis*. Mahwah: Erlbaum.

MacKinnon, D. P., Fritz, M. S., Williams, J., & Lockwood, C. M. (2007). Distribution of the product confidence limits for the indirect effect: Program PRODCLIN. *Behavior Research Methods, 39*(3), 384–389.

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication and Society, 19*(1), 111–126.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336–355.

Marangunić, N., & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society, 14*(1), 81–95.

Marx, G. T. (1999). What's in a name? Some reflections on the sociology of anonymity. *The Information Society, 15*(2), 99–112.

McCrae, R., & John, O. (1992). An introduction to the five-factor model and its applications. *Journal of Personality, 2,* 174–214.

Morio, H., & Buchholz, C. (2009). How anonymous are you online? Examining online social behaviors from a cross-cultural perspective. *AI & SOCIETY, 23*(2), 297–307.

Morosan, C., & De Franco, A. (2016). It's about time: Revisiting UTAUT2 to examine consumers' intentions to use NFC mobile payments in hotels. *International Journal of Hospitality Management, 53,* 17–29.

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review, 27*(4), 237–254.

Moyer, D., Carson, S. L., & Carson, R. T. (2015). Determining the influence of Reddit posts on Wikipedia pageviews. In *Ninth international AAAI conference on web and social media* (pp. 75–82). Oxford, UK: AAAI Press.

Müller-Seitz, G., Dautzenberg, K., Creusen, U., & Stromereder, C. (2009). Customer acceptance of RFID technology: Evidence from the German electronic retail sector. *Journal of Retailing and Consumer Services, 16*(1), 31–39.

Namara, M., Wilkinson, D., Caine, K., & Knijnenburg, B. P. (2020). Emotional and practical considerations towards the adoption and abandonment of VPNs as a privacy-enhancing technology. *Proceedings on Privacy Enhancing Technologies, 2020*(1), 83–102.

Nia, M. A., & Martínez, A. R. (2018). Systematic literature review on the state of the art and future research work in anonymous communications systems. *Computers & Electrical Engineering, 69,* 497–520.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

Norcie, G., Caine, K., & Camp, L. J. (2012). Eliminating stop-points in the installation and use of anonymity systems: A usability evaluation of the tor browser bundle. In *5th Workshop on hot topics in privacy enhancing technologies (HotPETS)*. Citeseer.

NortonLifeLock (2020, March 29). *2019 Cyber safety insights report global results*. Retrieved July 16, 2020 from, https://www.nortonlifelock.com/us/en/newsroom/press-kits/2019-norton-lifelock-cyber-safety-insights-report/.

O'Cass, A., & Fenech, T. (2003). Web retailing adoption: Exploring the nature of internet users web retailing behaviour. *Journal of Retailing and Consumer Services, 10*(2), 81–94.

Park, J., Gunn, F., Lee, Y., & Shim, S. (2015). Consumer acceptance of a revolutionary technology-driven product: The role of adoption in the industrial design development. *Journal of Retailing and Consumer Services, 26,* 115–124.

Pedeliento, G., Andreini, D., & Veloutsou, C. (2020). *Brand community integration, participation and commitment: A comparison between consumer-run and company-managed communities*. Journal of Business Research.

Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity—A proposal for terminology. In H. Federrath (Ed.), *Designing privacy enhancing technologies. Lecture notes in computer science* (Vol. 2009). Berlin: Springer.

Pizzi, G., & Scarpi, D. (2020). Privacy threats with retail technologies: A consumer perspective. *Journal of Retailing and Consumer Services, 56,* 102160.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879.

Reiter, M. K., & Rubin, A. D. (1998). Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security (TISSEC), 1*(1), 66–92.

Roßnagel, H. (2010). The market failure of anonymity services. In Chapter within, P. Samarati et al. (Eds.), *WISTP 2010, LNCS 6033* (pp. 340–354), 2010. IFIP International Federation for Information Processing.

Salimon, M. G., Yusoff, R. Z. B., & Mokhtar, S. S. M. (2017). The mediating role of hedonic motivation on the relationship between adoption of e-banking and its determinants. *International Journal of Bank Marketing, 35*(4), 558–582.

Sardá, T., Natale, S., Sotirakopoulos, N., & Monaghan, M. (2019). Understanding online anonymity. *Media, Culture and Society, 41*(4), 557–564.

Shatz, I. (2015). The negative impact of goal-oriented instructions. *Educational Studies, 41*(5), 476–480.

Shatz, I. (2016). Fast, free, and targeted: Reddit as a source for recruiting participants online. *Social Science Computer Review, 35*(4), 537–549.

Shaw, N., & Sergueeva, K. (2019). The non-monetary benefits of mobile commerce: Extending UTAUT2 with perceived value. *International Journal of Information Management, 45,* 44–55.

Shelton, M., Rainie, L. & Maddenn, M. (2015). *Americans' privacy strategies post-Snowden*, Pew Research Center's Internet and American Life Project. Retrieved July 16, 2020 from, https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/.

Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: Extending UTAUT with innovativeness, risk, and trust. *Psychology and Marketing, 32*(8), 860–873.

Spiekermann, S. (2005). The desire for privacy: Insights into the views and nature of the early adopters of privacy services. *International Journal of Technology and Human Interaction (IJTHI), 1*(1), 74–83.

Steenkamp, J. B. E., & Baumgartner, H. (1998). Assessing measurement invariance in cross-national consumer research. *Journal of Consumer Research, 25*(1), 78–90.

Stryker, C. (2012). *Hacking the future: Privacy, identity, and anonymity on the web*. ABRAMS.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics* (5th ed.). New York: Allyn and Bacon.

Tamilmani, K., Rana, N. P., & Dwivedi, Y. K. (2018a). Use of 'habit' is not a habit in understanding individual technology adoption: A review of UTAUT2 based empirical studies. In *IFIP 8.6 conference on smart working, living and organising*.

Tamilmani, K., Rana, N. P., Dwivedi, Y. K., Sahu, G. P., & Roderick, S. (2018b). Exploring the role of 'Price value' for understanding consumer adoption of technology: A review and meta-analysis of UTAUT2 based empirical studies. In *Twenty-second Pacific Asia conference on information systems Japan (PACIS)*.

Tamilmani, K., Rana, N. P., Prakasam, N., & Dwivedi, Y. K. (2019). The battle of Brain vs. Heart: A literature review and meta-analysis of "hedonic motivation" use in UTAUT2. *International Journal of Information Management, 46,* 222–235.

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology, 52*(5), 463–479.

Udo, G. J. (2001). Privacy and security concerns as major barriers for e-commerce: A survey study. *Information Management and Computer Security, 9*(4), 165–174.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36,* 157–178.

Wallace, K. A. (2008). Online anonymity. In K. E. Himma & H. T. Tavani (Eds.), *The handbook of information and computer ethics* (p. 165). New York: Wiley.

Weiss, L. M., Capozzi, M. M., & Prusak, L. (2004). Learning from the internet giants. *MIT Sloan Management Review, 45*(4), 79.

West, S. M. (2019). Data capitalism: redefining the logics of surveillance and privacy. *Business & Society, 58*(1), 20–41.

Whitten, A., & Tygar, J. D. (1999). Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium* (Vol. 348, pp. 169–184).

Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets, 19*(2–3), 137–149.

Zuboff, S. (2015). Big Other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(75), 89.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in publishedmaps and institutional affiliations.