Decision Support Systems 56 (2013) 103–114

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context

Caroline Lancelot Miltgen [a,*], Aleš Popovič [b], Tiago Oliveira [c]

[a] GRANEM, Faculty of Law, Economics and Business, University of Angers, LUNAM, France
[b] Faculty of Economics, University of Ljubljana, Slovenia & ISEGI, Universidade Nova de Lisboa, Lisboa, Portugal
[c] ISEGI, Universidade Nova de Lisboa, Lisboa, Portugal

ARTICLE INFO

Article history:
Received 28 June 2012
Received in revised form 27 April 2013
Accepted 15 May 2013
Available online 26 May 2013

Keywords:
Biometric system
Technology acceptance
Privacy
Risk
Trust
Personal data

ABSTRACT

The information systems (IS) literature has long emphasized the importance of user acceptance of computer-based IS. Evaluating the determinants of acceptance of information technology (IT) is vital to address the problem of underutilization and leverage the benefits of IT investments, especially for more radical technologies. This study examines individual acceptance of biometric identification techniques in a voluntary environment, measuring the intention to accept and further recommend the technology resulting from a carefully selected set of variables. Drawing on elements of technology acceptance model (TAM), diffusion of innovations (DOI) and unified theory of acceptance and use of technology (UTAUT) along with the trust-privacy research field, we propose an integrated approach that is both theoretically and empirically grounded. By testing some of the most relevant and well-tested elements from previous models along with new antecedents to biometric system adoption, this study produces results which are both sturdy and innovative. We first confirm the influence of renowned technology acceptance variables such as compatibility, perceived usefulness, facilitating conditions on biometrics systems acceptance and further recommendation. Second, prior factors such as concern for privacy, trust in the technology, and innovativeness also prove to have an influence. Third, unless innovativeness, the most important drivers to explain biometrics acceptance and recommendation are not from the traditional adoption models (TAM, DOI, and UTAUT) but from the trust and privacy literature (trust in technology and perceived risk).

1. Introduction

Information technology (IT) acceptance and use has been one of the priority issues of information systems (IS) research and practice since the late 1980 [84,88]. IT is becoming increasingly complex and crucial for business operations, thus making the issue of acceptance an important challenge in IT implementation. Despite impressive advances in technology capabilities, the problem of underutilization of IT, especially for more radical technologies, is still present [3]. To leverage the benefits of IT investments, firms increasingly show interest in factors facilitating the implementation success, in particular factors affecting technology acceptance. Driven by extensive research to understand IT acceptance [87,88] therefore, different models and theories that incorporate a variety of social, behavioral and other control factors were developed in the past to explain IT usage (i.e. [21,84,87,88]).

In personal identification and authentication field, the application of biometric technologies is increasingly apparent [75]. Practical evidence shows that augmented interest in these technologies is fuelled by anticipated decrease of technology costs, improved technical quality of the systems and socio-political pressures for better security-related controls [71]. Nevertheless, an important issue stemming the deployment of biometrics or leading to their underutilization is user resistance to utilize such pervasive technology [71]. Most users feel fearful, hesitant, or uncomfortable around these systems especially because they perceive them as means for potential infringements into their privacy [75]. Such users' feelings and perceptions increase the risk of rejection and can lead to biometrics implementation failure [71]. The need to inform biometric technologies implementation with various factors affecting biometrics acceptance is, therefore, of crucial importance [63,71].

To date, only a few authors have discussed biometric systems from a consumer acceptance perspective [63]. Yet, the perception and behavioral response of end users are important considerations when designing systems that employ digital identities [44] as issues of privacy, security and online identity management are frequently a source of concern to consumers [22]. A study aiming to identify relevant non-technical issues such as the perceptions of future end-users' fears and anticipations is likely to be a prerequisite for the development of a strategy to support the acceptance of such a pervasive innovation. Biometrics has often been associated in the

* Corresponding author at: GRANEM, Faculty of Law, Economics and Business, 13 Allée François Mitterand, 49036 Angers Cedex 01, France. Tel.: +33 665 012 704.
E-mail address: caroline.miltgen@orange.fr (C. Lancelot Miltgen).

0167-9236/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2013.05.010

popular press at least – and in the public consciousness Ng-Kruelle et al. [64] argue – with the encroachment of state control through technologies. The citizens may on the whole have become educated to the necessity of increased security but it is not clear that there is general acceptance that associated intrusions on their privacy are either a necessary or an appropriate price to pay for it. This study will therefore address the following research question: What are the key determinants of end-user acceptance (or reject) of some disruptive IT like biometric systems in voluntary environments?

Although isolated impacts of technical, social, and risk factors on intention to accept IT have been well documented within existing IT acceptance models (i.e. [24,41,100]), a more comprehensive understanding regarding the various factors explaining IT acceptance, is needed. This isolated approach limits the ample view of different factors that organizations trying to succeed with IT implementation have to carefully address in order for the target users to accept the IT under investigation. To address this gap we explored how an interplay of previously identified factors from existing IT/IS acceptance models and theories adds to the richness of explaining biometric technology acceptance among digital native end-users.

Our contribution to the IT acceptance literature is threefold. Firstly, our results highlight the relative importance of diverse drivers and individual, technical, social, and risk determinants in explaining the intention to accept biometric technologies. To date, rather limited attention has been paid to technology-specific antecedents that may provide significantly stronger guidance for the successful design and implementation of specific types of systems. Therefore, in addition to classical antecedents to IT acceptance, we incorporate particular factors linked with the specificities of biometric systems. Developing theory that is more focused and context specific – here, technology specific – is considered an important frontier for advances in IS research [68,84]. Such comprehensive and focused model appears be more explanatory compared to a general model that attempts to address many classes of technologies [84] and should also provide designers with levers to augment adoption.

Secondly, we identify that through integration of different IT acceptance models and some other theories we are able to provide a better picture of IT acceptance antecedents and their relationships. As such, privacy concerns are an important consideration in successful biometric implementation and uptake among citizens [75]. Although the issue of privacy has emerged as a major inhibitor of biometrics acceptance [75], however, the research on this issue is quite rare to date, especially from the viewpoint of customers. A model that integrates knowledge from technology adoption and privacy research and which encompasses both privacy and trust as components central to effective acceptance [75] is clearly lacking, a gap that this paper seeks to address. In doing so, we answer the call from Venkatesh et al. [87] to integrate the technology adoption stream with another dominant research stream, which in turn will move us toward a more cumulative and expansive nomological network (see [84]).

Lastly, although not directly reflected in our model, we explore IT acceptance determinants in voluntary environments. While voluntariness is an important dimension in technology acceptance literature [86,87,95], for biometric systems in particular, the examination of acceptance in voluntary settings remains more challenging compared to mandatory settings. Focusing upon potential future end-users of biometrics – all having complete volitional control over using or not using the technology – such investigation may provide very important insight into the free formation of attitudes and intentions to use new technologies [63].

In the next section we develop the conceptual research model and then outline the sources of data and our data analysis procedure. This is followed by a description of the role of the different factors explaining the intention to accept biometrics. We then discuss the theoretical contributions and managerial implications of our findings. The paper concludes with avenues for future research.

2. Model development

2.1. The biometric identification systems

Biometric identification systems recognize and authenticate people based on a person's unique physical or behavioral features. Consumer-oriented biometric systems have been sporadically adopted in the past; yet, their application has been steadily increasing in recent years. Retailers and service providers throughout the World implement biometric technologies to offer their customers increased levels of convenience and access to customer-restricted facilities [38,59,92]. Although authorities and organizations do not always a priori care for the opinions of the general public about biometric technologies, they are often compelled to do so since the acceptance of such technologies by the general public is indeed a clear step toward the success of the implementation [80]. The consequences of not addressing potential pressures from the general public might easily lead to implementation failures (e.g. in 2007 Serbians pressed the Serbian government to back off on a plan to make biometric data compulsory in the country's new ID cards, in 2012 Newcastle University students vote against biometrics to track course attendance).

The most notable biometric technologies already in use for the identification of people are face recognition, fingerprints, iris recognition, hand geometry, and voice recognition [77]. According to Uludag et al. [82], the security issues regarding biometric implementations are much more complex than with any other IT system. Although no biometric system offers complete security [35], studies indicate that high-priced systems, such as iris scanners, are more effective and less likely to make false identifications than cheaper systems like signature dynamics [79]. As a range of technologies which identify the individual, either accurately or inaccurately, and with or without their knowledge and consent, biometric identification systems have potential to both enhance and threaten privacy and it is the security of the whole system which leads to potential privacy risks or protection.

As noted by Shaikh & Rabaiotti [77], one of the primary applications of biometric-based identity management is for 'identity verification and law enforcement' by governments and national agencies. As these technologies are becoming more familiar to the general public, organizations in the private sector are increasingly adopting them as well [19]. Yet, there is substantial evidence that, over the past decades, people globally have become less confident in and more cynical of their governments and private companies [67] which want to implement technologies that increase dataveillance on their employees, customers and the general public. Technology acceptance, however, depends on the characteristics of both the technology in question and the adopting units [41]. Regarding the former, the key factor is the content/utility of the technology. Regarding the characteristics of the adopting unit, technology acceptance is shaped by three sets of variables, namely exposure, capacity to adopt and use, and state policies [41].

2.2. Theoretical frameworks of technology acceptance

Theoretical frameworks of technology acceptance are IS theories that model how users come to accept and use a specific technology. These theories suggest that when users are presented with a new technology, a number of factors influence their decision about how and when they will use it. The technology acceptance model (TAM) [21] provides a seminal framework for this study. Since the early stages of its conception, there have been many improvements and/or extensions to the TAM, as well as the development of other models which also take into consideration the potential influence of technological elements. Despite its simplicity (which can also be considered as valuable parsimony) and contentiousness, TAM has proven particularly useful in studying the intent to accept new IT in a wide variety of contexts, such as across US companies [87], among college students shopping

online [37], in regards to internet banking [99], e-procurement [1], or electronic toll collection service [11]. However, because TAM seems to neglect some individual factors that could influence user preferences in the acceptance of the technology, some additional individual variables as well as a more integrative view of the antecedents of technology acceptance are needed. The motives underlying the acceptance of biometrics indeed introduce additional significant constructs (like variables linked with privacy issues), which cannot be explained or satisfactorily dealt with by existing theoretical frameworks or adoption models individually. It is therefore proposed that an integrated theoretical framework, which can be used in evaluating the facilitators and inhibitors of biometrics success, can be created from a synthesis of the relevant constructs of existing theories and best practices in TA. In addition to the TAM model therefore, two widely-used technology acceptance (TA) models would be used in this paper. Firstly, diffusion of innovations (DOI) theory purports to contribute to the accuracy of models by examining innovations and the success of their dissemination through a more accurate indicator of consumer behavior [74]. Secondly, variables from the integrated unified theory of acceptance and use of technology (UTAUT) framework bring additional insights into the study of biometrics acceptance.

2.3. Prior, antecedents and consequences factors to biometric acceptance

In the recent technology acceptance literature, central to efforts of extending technology acceptance/adoption frameworks is the call for incorporating consumer perceptions of unique, contextually relevant innovation characteristics along with personal characteristics in studying consumers' innovation-acceptance phenomena [62]. In our model, we thus examine joint influence of combined DOI, TAM and UTAUT constructs with other situational and technology-specific characteristics to explain consumers' intention to use biometrics. The variables included in these three seminal models mostly focus on the perceived benefits of the technology to adopt. As our research aims to have direct relevance to the real-world issues of technology acceptance and resistance we want to target both the particular enablers and barriers to the adoption of these technologies and therefore also included the perceived negatives of biometrics such as the perceived risks. In addition, because all benefit and cost components that help explain technology acceptance and resistance are themselves determined by independent variables, the model also account for prior factors such as individual's innovativeness, trustworthiness, and privacy concerns.

Many authors have studied different aspects of new technology acceptance from a variety of theoretical perspectives, including TAM, DOI and UTAUT. In each of these theories, behavior (e.g., the use of biometric system) is viewed as the result of a set of beliefs about technology and a set of affective responses to the behavior. Behavioral intentions to accept a new technology have been shown to be reliable predictors of customer acceptance rates across a wide range of domains and provide efficient means of assessing behavioral outcomes [37]. Measuring intention to accept a new technology can thus be seen as an effective way to evaluate the potential success of the system and is, as such, central to our investigation and one key dependent variable of our conceptual framework. While expanding the evaluation of the success of a new technology beyond mere usage represents one of the areas of IS field still lacking systematic investigation [45], our model also includes consumer's intention to recommend a technological innovation as a possible way to evaluate the success of a new technology. Recommending a technology to others is a post-adoption behavior that is often of great commercial interest to providers (Chung and Shin 2010), but has often been neglected by researchers due to an overwhelming emphasis on use. We may also recognize today that technology acceptance can have more than individual significance, as social networks provide new routes for influential dissemination of attitudes and even behaviors. Therefore, this research includes intention to recommend as a second key dependant variable.

In order to assess the presented behavioral outcomes we take a two-phase approach to model development. Firstly, grounded in technology acceptance/adoption frameworks of TAM, DOI and UTAUT, we propose factors that are able to influence the beliefs about behavioral intention to use biometrics. The beliefs are represented by perceived usefulness and perceived ease of use in TAM, by the perceived characteristics of innovating in DOI research, and by outcome expectations in UTAUT. They have been referred to as the net benefits (realized or expected) accruing from use of the technology [76]. However, while the TAM and DOI perspectives focus almost exclusively on beliefs about the technology and the outcomes of using it, UTAUT includes other beliefs that might influence behavior, independent of perceived outcomes. In our study, the well-tested TAM constructs of PU and PEOU are chosen rather than the similar DOI constructs of relative advantage and complexity because TAM remains the bedrock of our framework. Some DOI constructs are not well-suited to our model as biometrics has not yet been thoroughly implemented in practice. The trialability and observability constructs are consequently not introduced in our framework as the majority of the people surveyed will probably not have tested these technologies yet. As a result, the only DOI variable we have incorporated into our model is that of 'compatibility' of the innovative technology. The UTAUT model incorporates the notion of social influence as an independent influence on behavior and also gives prominence to the concept of facilitating conditions. The addition of social influence to our model is critical to the recognition that adoption is not just about convincing people of the benefits to be derived from a technology (selling the technology), but it must also be about identifying individuals with strong personal influence (formal and informal) and work with them to become advocates for technology use in order to facilitate the implementation process. Adequate facilitating conditions (continuous training and technical support to users) should also play an important role in biometrics intention to use. Again, we have chosen not to include the UTAUT variables of 'performance expectancy' and 'effort expectancy' because these variables were considered too similar to the TAM variables of 'perceived usefulness' and 'perceived ease of use'.

Secondly, despite the vigor of technology acceptance/adoption frameworks, some researchers indeed suggest that other prior factors may importantly influence attitudes toward using a technology [32,69]. Most privacy studies show that consumers' acceptance or reluctance to disclose personal data is attributable to corresponding differences in the perceived severity of negative consequences of disclosure, i.e. risks [72]. Perceived risks are linked to particular decisions (for example, the decision to self-disclose), which occur in specific circumstances. For biometric systems, psychological (i.e. privacy and identity) risks are usually considered important [81]. Next, many empirical studies have already incorporated trust into TAM (e.g. [33]), DOI (e.g. [9]) and UTAUT (e.g. [40]) models based on the idea that trust in the implemented technology leads to greater efficiencies in acceptance by promoting an environment that is conducive to technology acceptance. Both because of the dominance of trust in the existing literature, and because biometric system demands the cooperation of individuals with little ability to monitor or control those operating it, trust is an important factor when considering biometric technology acceptance. Moreover, numerous studies have consistently concluded that an overwhelming majority of people are 'concerned' or 'very concerned' about threats to their privacy, and are willing to act to protect it [18]. Privacy concern has been shown to be associated with elevated levels of perceived risk in relation to technology acceptance [81]. Indisputably, privacy concerns are a primary reason for the public fears about accepting biometric technologies as well, since biometric data is highly personal and offers a potential privacy invasion deriving from the tight link between the owner's identity and body. Finally, we reasoned that a person who tends to be innovative will be more likely to take on new challenges than others. Based on previous findings that indicate innovativeness significantly predicts intention to accept an IT system [40], we included innovativeness in our model.

The conceptual model used to guide the study is shown in Fig. 1. The model identifies the linkages between prior factors (such as innovativeness, trust and privacy concerns), antecedent factors, such as beliefs about the technology, and other variables such as social influence and facilitating conditions, and the two consequent factors of intentions to accept and to recommend using the biometric system.

2.3.1. The impact of TAM variables on behavioral intention to accept a biometric system

TAM proposes perceived usefulness (PU) [4,13,97] and perceived ease of use (PEOU) determine intention to accept a technology [21,46]. Empirical evidence has shown that PEOU does have an effect on intention to accept not only directly but also indirectly through PU [23,31,86]. In this light we anticipate the same to be true in the case of acceptance of the biometric technology.

H1. The greater the perceived usefulness, the greater the intention to accept a biometric system.

H2. The greater the perceived ease of use, the greater the intention to accept a biometric system.

H3. The perceived usefulness of the biometric system is positively correlated to perceived ease of use.

2.3.2. The impact of DOI variables on behavioral intention to accept a biometric system

Studies on innovation diffusion and technology acceptance suggest that compatibility is another important variable in determining technology acceptance outcomes (e.g. [2,48,96,98]). As Wang & Liao [90] recognized, a strong (and often neglected) relationship also exists between compatibility and perceived ease of use. Compatibility has also been shown to contribute significantly to the accurate prediction of acceptance intent [9]. The research of Koenig-Lewis et al. [49] acknowledges that compatibility not only had a strong direct effect but was also identified as an important antecedent for perceived ease of use and perceived usefulness. Greater compatibility therefore denotes a synergy between biometric system and the customer's social and cognitive skills, which reinforced both the perceived usefulness and ease of using a technology.

H4a. The greater the perceived compatibility, the more likely a customer will perceive a biometric system as useful.

H4b. The greater the perceived compatibility, the more likely a customer will perceive a biometric system as easy to use.

However, as the general public is relatively unfamiliar with biometric systems, we anticipate this system will not be perceived as highly compatible with existing technologies and this will dampen acceptance intent.

H5. The greater the perceived compatibility, the greater the intention to accept the biometric system.

2.3.3. The impact of UTAUT variables on intention to accept biometric system

López-Nicolás et al. [58] defined social influence as the degree to which individuals believed that others thought they should use the technology. In our study, we will also consider social influence to be related to notions of peer pressure in the context of the biometric technology acceptance. We expect social influence will have an effect on behavioral intention, a causal link previously already modeled [16]. Social influence may conceivably have a negative effect on intention to accept [39], as the threats of biometrics are well-known and are embedded into national psyches. Alternatively, among the younger generation it is quite possible that technological intrusion into an individual's personal life is perceived as normal, fostering acceptance by becoming the 'subjective norm' [98]. As social influence can both encourage and discourage acceptance, our hypothesis postulates that it is the degree to which a social circle perceives the technology to be normal which directly correlates to technology acceptance.

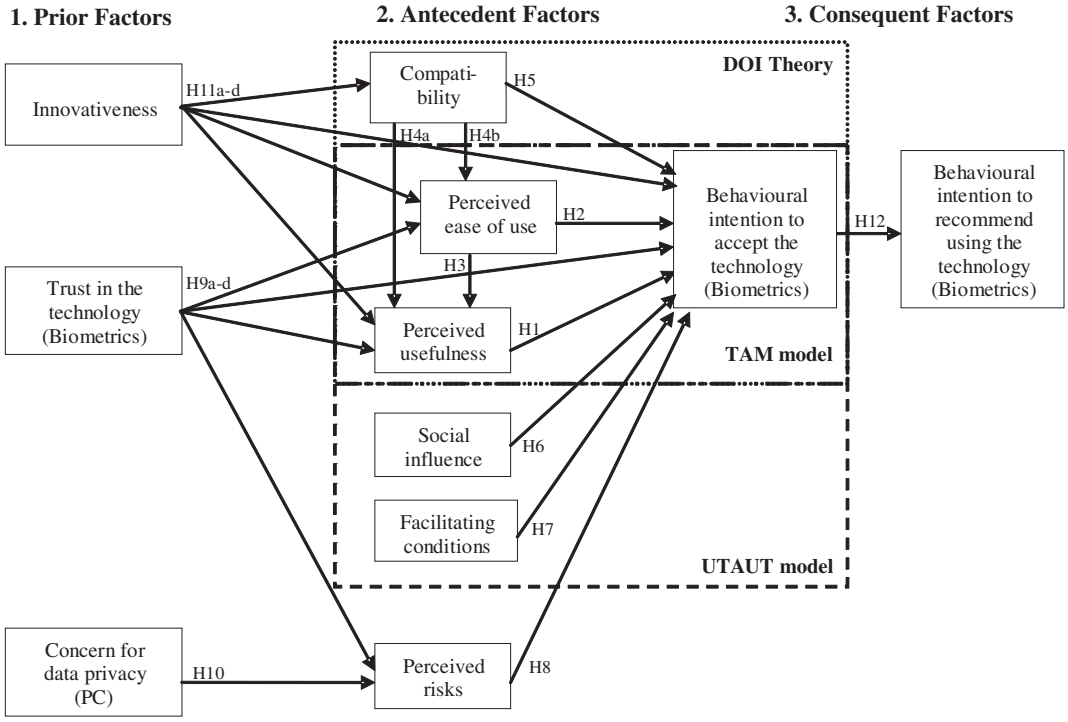

Fig. 1. Proposed theoretical framework.

H6. Social influence will have a strong impact on consumer intentions to accept a biometric system: the extent to which a biometric system is perceived as 'normal' by an individual's social circle will have a positive relationship to their intention to accept it.

Facilitating conditions are usually defined as 'the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system' [87]. In our work, as we study the general public's intention to accept biometric systems for 'current use' and not for a use specific to any organizational context, facilitating conditions will refer to 'whether an individual believes that some enabling factors exist to support acceptance of the system'. We hypothesize, alongside some of our contemporaries (e.g. [16]), a causal link exists between facilitating conditions and users intentions, so that greater facilitating conditions will increase the likelihood to accept biometrics.

H7. Facilitating conditions will have a positive influence on consumer intentions to accept biometric system.

2.3.4. The impact of perceived risks on intention to accept biometric system

Consumers are highly concerned by the different types of risks that confront them, even when the technology involved has a better privacy reputation than biometric technology [96], and it has already been shown that heightened risk perceptions are associated with lower consumer intentions to adopt [48,56]. In our study it is expected that perceived risk, which in all likelihood will be higher for biometric technology than for other forms of electronic identification, will lower consumer intentions to tolerate this new technology [55,78].

H8. The greater the perceived risks, the lesser the intention to accept a biometric system.

2.3.5. The antecedents of beliefs (prior factors)

2.3.5.1. The influence of trust. Trust is one of the most effective tools for reducing uncertainty [6], the sense of risk and generating a sense of safety [69] and consumer trust is believed to play a pivotal role in consumers' intentions to accept a biometric system [9] by reducing the perceived risks [48] and uncertainty associated with the acceptance [69]. As trust increases, consumers are likely to perceive less risk than if trust were absent; the effect of trust on the consumer's intention to accept biometric technologies is thus mediated by risk as already suggested by [47].

H9a. Consumer trust in the technology has a negative impact on consumer perceptions of risk when accepting a biometric system.

Trust in the technology does not only influence the perceived risks associated with accepting the technology but is also an antecedent of ease of use [69] and usefulness [51]. TT encourages a user to accept a technology when he is apprehensive about doing so, which often leads to circumstances whereby he can learn the benefits and usefulness of the new product or service. Moreover, TT will make the product easier to use, as the trust will lower psychological costs associated with accepting the new technology [50].

H9b. Consumer trust in the technology has a positive impact on the perceived usefulness (b) and on the perceived ease of use (c) of a biometric system.

Previous research has also hypothesized that trust is directly significant in shaping a consumer's intention to accept a technology (e.g. [9,31]). As some scholars stated explicitly, trust has a direct influence on behavioral intention to use [94]. We anticipate therefore that the elements of trust in the biometric system increase a customer's disposition to accept this technology, and therefore trust should also influence behavioral intention directly.

H9d. Consumer trust in the technology has a positive impact on intention to accept a biometric system.

2.3.5.2. The influence of privacy concerns. Identity theft has become both easier and more efficient in the digital age and this often leads to fraud [26]. Consumers who do business with organizations are highly concerned and vulnerable as their personal data can be compromised and misused. These growing privacy concerns have led to an even greater emphasis on risk perception in decision-making as regards data disclosure [102]. Therefore, consumers with higher privacy concerns will perceive higher risks in giving their personal identity. As the biometric system inherently requires personal data to be used, the following hypothesis is proposed.

H10. Consumers with higher privacy concerns will perceive accepting a biometric system to be riskier.

2.3.5.3. The influence of innovativeness. Innovativeness has been shown to be a significant direct predictor of behavioral intention to use new technologies [98]. However, it has also been suggested that individual innovativeness might be a predictor of the TAM and DOI variables (e.g. [8,73]). Yi et al. [98] confirm that, regardless of the measure or the innovation acceptance settings, the disposition towards innovativeness directly determines three characteristics, namely perceived usefulness, ease of use and compatibility.

H11. Consumers with higher personal innovativeness are more likely to perceive the technology characteristics of usefulness (a), ease of use (b) and compatibility (c) more positively and to be willing to accept biometrics (d).

2.3.6. Influence on consumers' intention to recommend the technology

If consumers are usually swayed by word-of-mouth when judging the quality of an innovation [85], they are also capable of contributing their own opinions to the discourse. Literature exploring the relationship between behavioral intentions and actions notes that consumers with a higher intention to accept a new technology are very much more likely to become adopters of the technology [53], and then often recommend the technology to others [57]. As suggested by Goldsmith & Flynn [34], consumers' high acceptance intention can influence the intention to recommend the technology to their social network. Therefore, and backed up by existing works (e.g. [61]), we feel confident theorizing a causal link between behavioral intention to accept biometrics and the intention to recommend using it to others.

H12. The intention to accept the biometric system positively influences the intention to recommend this technology to others.

3. Method and sample

As we primarily intend to investigate the actual and future attitudes and behaviors of the youngsters as regards biometrics (and the iris scanning technology in particular), an online survey has been devised because it appears the quicker and more pertinent way to obtain their opinions. It uses a scenario method whereby respondents are presented with a written scenario (Appendix A) describing a simulated situation, in which a friend has the opportunity to accept a specific biometric application to identify him/herself before a driving test. This approach is suitable for eliciting beliefs and reactions in typical situations, especially in relation to moral dilemmas. Hypothetical scenarios have been used in a range of technology research, especially in technology acceptance studies [12].

A preliminary questionnaire was presented and discussed during a workshop. On the basis of the recommendations received from peers, a revised version of the questionnaire was devised and tested through a small-scale field trial (pre-test) which enrolled 117 young people in the United Kingdom (UK). The results of this pre-test were used to amend, remove and reformulate some questions. Emails with invitations to participating to the final survey were sent to people, retrieved from a selected sample from a Net Surfers database managed by the 1000mercis French company through its Elisa program. The sample for our survey was selected in the Elisa database by using quotas, based on Eurostat data. In particular, the two criteria that were used to discern possible participations in line with demographic data were: gender (male/female) and age (split into two groups 15–18 year olds and 19–25 year olds). This sampling method should implicate the relative representativeness of the sample based on the above criteria.

We obtained 326 young (15–25 years old) respondents for a response rate of 48%. 67% of the respondents were male and 33% female. Those surveyed were generally at the older end of the specified age range. The largest sub-section of respondents came from the student community, with some at BA level (20%), some at MA level (13.5%) and some at PhD level (3%). Most of those surveyed were experienced with the internet: 91% have broad band at home; 77% use internet more than five years; and 80% use it several times a day. Appendix B presents the sample characteristics.

Participants in the study are thus diverse in gender and education level and we can assume to say that our sample is not specifically atypical (e.g. all middle class participants). The findings presented here can thus be taken to indicate current young European citizens' attitudes towards technology adoption and the acceptance of a specific biometric identification system in particular.

To test our conceptual framework, major constructs with multi-item scales (Appendix C) were measured. As the questionnaire was very long, and in order to decrease any bias in the answers due to the respondents' fatigue, the shortest scales found in the orthodox literature were applied and the minimum number of items were retained (e.g. only two items are used for trust in the technology). Some variables – social influence and recommendation intention – are measured in one single item. To ensure their content validity, all scales were pre-tested and validated by peers.

4. Data analysis and results

To analyze the relationships defined by our research model it was applied a structural equation model. As all items in our data are not distributed normally ($p < 0.01$ based on Kolmogorov–Smirnov's test) and the research model is complex, the partial least squares (PLS) is the most adequate method in this case [14,15].

PLS factor loadings, average variance extracted (AVE), composite reliability (CR), and Cronbach's alpha are presented in Table 1. All items have loadings greater than 0.7, except PU1 which is close to this cut-off criteria (0.68). All the items are statistically significant at the 0.01 level (t-statistics obtained from bootstrapping with 500 resamples), suggesting good convergent validity [30]. Most constructs have CR and alphas above the recommended value of 0.7 [66] suggesting good reliability.

Discriminant validity of the constructs was assessed using two measures: Fornell–Larcker criteria and cross-loadings. The first criterion postulates that the square root of AVE should be greater than the correlations between the construct [30]. The second criterion requires that the loading of each indicator should be greater than all cross-loadings [14]. As seen in Table 2, the square roots of AVEs (diagonal elements) are higher than the correlation between each pair of constructs (off-diagonal elements). The loading and cross-loading tables (available from the authors on request) show that the patterns of loadings are greater than cross-loadings. Thus both measures are satisfied.

Table 1
Factor loadings, average variance extracted, composite reliability and alphas.

Factor	Item	Loading	t-Value	AVE	CR	Alpha
Perceived usefulness (PU)	PU1	0.68	13.16***	0.59	0.81	0.66
	PU2	0.82	28.97***			
	PU4	0.80	26.18***			
Perceived ease of use (PEOU)	PEOU3	0.98	256.55***	0.96	0.98	0.96
	PEOU4	0.98	264.85***			
Compatibility (Comp)	Comp1	0.93	86.87***	0.86	0.95	0.92
	Comp2	0.95	134.28***			
	Comp3	0.90	55.37***			
Facilitate conditions (FC)	FC1	0.90	29.52***	0.84	0.91	0.81
	FC3	0.93	57.97***			
Perceived risks (PR)	PR1	0.74	22.00***	0.71	0.96	0.95
	PR2	0.81	33.18***			
	PR3	0.86	46.18***			
	PR4	0.84	39.89***			
	PR5	0.81	31.61***			
	PR6	0.82	43.06***			
	PR7	0.92	98.94***			
	PR8	0.93	104.92***			
	PR9	0.87	44.33***			
Trust technology (TT)	TT1	0.96	154.22***	0.91	0.95	0.90
	TT2	0.95	126.81***			
Privacy concerns (PC)	PC1	0.81	22.24***	0.72	0.94	0.92
	PC2	0.90	59.41***			
	PC3	0.90	61.77***			
	PC4	0.80	25.09***			
	PC5	0.80	21.73***			
	PC6	0.88	56.47***			
Innovativeness (Innov)	Innov1	0.87	38.95***	0.83	0.94	0.90
	Innov2	0.92	54.99***			
	Innov3	0.93	81.68***			
Behavioral intention (BI)	BI1	0.97	191.12***	0.93	0.96	0.93
	BI2	0.96	170.58***			

Note. PU3, PEOU1, PEOU2, FC2, FC4, and BI3 items were excluded due to poor loadings.
*** $p < 0.01$.

In summary, our model has good convergent validity, reliability and discriminant validity. Consequently, constructs developed by this measurement model could be used to test the research model. Table 3 summarizes the results of PLS estimation. The model explains 42% of behavioral intention (BI) to accept biometrics (iris recognition) and, most hypotheses (i.e. H1, H5, H7, H8, H9d and H11d) are confirmed with only hypotheses H2 and H6 not verified at all. The model explains 19.3% of perceived usefulness (PU) as only the compatibility hypothesis (H4a) is validated. The model explains 33.9% of perceived ease of use (PEOU), the hypotheses of compatibility (H4b) and innovativeness (H11b) being corroborated. 12.6% of perceived risks (PR) are explained by the model and the privacy concerns hypothesis (H10) is approved. Innovativeness influence on compatibility (H11c) is also confirmed explaining 5.7% of this construct. Behavioral intention hypothesis (H12) is also validated and explains 42% of recommendation. Overall, of the 12 hypotheses formulated (19 if we count the sub-hypotheses), 7 are confirmed by the data (12 out of the 19 sub-hypotheses).

As the goal of this research is to understand the determinants of end-user acceptance of biometric systems in volitional environments, we will now focus our analysis on the main drivers of acceptance and recommendation. The main facilitators of BI are trust in technology (TT) ($\hat{\beta} = 0.246$; $p < 0.01$), followed by innovativeness (Innov) ($\hat{\beta} = 0.208$; $p < 0.01$), perceived usefulness (PU) ($\hat{\beta} = 0.202$; $p < 0.01$), compatibility (C) ($\hat{\beta} = 0.145$; $p < 0.10$) and facilitating conditions (FC) ($\hat{\beta} = 0.103$; $p < 0.05$). The main inhibitor of BI is perceived risks (PR) ($\hat{\beta} = -0.106$; $p < 0.01$). The results thus show that TT is the most important construct in explaining BI. What first drives biometrics acceptance therefore is the

Table 2
Matrix of correlation constructs and the square root of AVE (in bold).

	PU	PEOU	Comp	SI	FC	PR	TT	PC	Innov	BI	REC
Perceived usefulness (PU)	**0.77**										
Perceived ease of use (PEOU)	0.10	**0.98**									
Compatibility (Comp)	0.41	0.57	**0.93**								
Social influence (SI)	0.37	−0.01	0.27	**na**							
Facilitate conditions (FC)	0.42	0.10	0.29	0.39	**0.92**						
Perceived risks (PR)	−0.06	0.22	−0.04	−0.18	−0.07	**0.84**					
Trust technology (TT)	0.33	0.50	0.82	0.30	0.28	−0.11	**0.95**				
Privacy concerns (PC)	0.04	0.08	−0.11	−0.12	0.02	0.35	−0.13	**0.85**			
Innovativeness (Innov)	0.05	0.24	0.24	−0.05	−0.01	0.10	0.18	0.00	**0.91**		
Behavioral intention (BI)	0.42	0.27	0.53	0.30	0.33	−0.15	0.53	−0.13	0.28	**0.97**	
Recommendation (REC)	0.50	0.09	0.38	0.36	0.45	−0.24	0.38	−0.08	0.09	0.65	**na**

Note: na — average variance extracted are not applicable to the single-item constructs; the constructs are standardized (mean 0 and standard deviation 1).

trust users have in this specific technology followed by users' own interest in trying new technologies.

Since direct effects may not necessarily be comprehensive enough, the study extends to identify the total effect of independent variables (see Appendix D). This total effect is particularly relevant to more exhaustively understand recommendation as there is merely a single direct effect in this case. To explain the biometrics' recommendation, besides the direct effects of BI, we also considered total effects. By doing this, we found that the total effect of perceived usefulness (PU) on recommendation is 0.131 (0.202 ∗ 0.648). This means that PU is relevant not only to explain BI, but also to explain recommendation. The positive predictors of recommendation therefore are innovativeness (0.165), trust in technology (0.161), compatibility (0.153), PU (0.131), and facilitating conditions (0.067). On the other edge of the spectrum, as negative influencers we have the total effect of perceived risks (−0.068), and concern for data privacy (−0.023).

Table 3
Results for the structural model and hypothesis testing.

Path	β	t-Value	R^2	Hypothesis (confirmations)
Behavioral intention (BI)			42.0%	
Perceived usefulness (PU)	0.202	4.192***		H1 (yes)
Perceived ease of use (PEOU)	0.005	0.084		H2 (no)
Compatibility (C)	0.145	1.765*		H5 (yes)
Social influence (SI)	0.061	1.303		H6 (no)
Facilitate conditions (FC)	0.103	2.338**		H7 (yes)
Perceived risks (PR)	−0.106	2.122**		H8 (yes)
Trust technology (TT)	0.246	3.318***		H9d (yes)
Innovativeness (Innov)	0.208	4.098***		H11d (yes)
Perceived usefulness (PU)			19.3%	
Perceived ease of use (PEOU)	−0.190	2.298**		H3 (no)
Compatibility (C)	0.529	5.837***		H4a (yes)
Trust technology (TT)	−0.007	0.089		H9b (no)
Innovativeness (Innov)	−0.031	0.616		H11a (no)
Perceived ease of use (PEOU)			33.9%	
Compatibility (C)	0.469	5.939***		H4b (yes)
Trust technology (TT)	0.094	1.166		H9c (no)
Innovativeness (Innov)	0.108	2.184**		H11b (yes)
Perceived risks (PR)			12.6%	
Trust technology (TT)	−0.071	1.155		H9a (no)
Privacy concerns (PC)	0.338	5.862***		H10 (yes)
Compatibility (Comp)			5.7%	
Innovativeness (Innov)	0.239	4.592***		H11c (yes)
Recommendation (REC)			42.0%	
Behavioral intention (BI)	0.648	18.467***		H12 (yes)

Note: β: standardized coefficients. The constructs are standardized (mean 0 and standard deviation 1).
* $p < 0.10$.
** $p < 0.05$.
*** $p < 0.01$.

These results reveal that unless innovativeness the most important drivers to explain biometrics acceptance and recommendation are not from the traditional acceptance models (TAM, DOI, and UTAUT), but from the trust and privacy literature (trust in technology and perceived risk). These new variables, included in our model, to explain biometrics intention and recommendation are in fact more important than PEOU used in TAM or social influence from UTAUT.

5. Discussion

5.1. Theoretical implications

Despite increasing recognition of the effect that different factors may exert on acceptance of biometric systems, this influence has been under-researched until now. There is a lack of explanatory models and empirical and theory-building studies on the above mentioned research field. Filling this gap is important, in relation to both theory and practice. This study sheds some light on this area of research.

Our research contributes to the general IT and specific biometric systems acceptance body of research by (1) being – to our best knowledge – one of the first study in this biometric field aiming to identify relevant non-technical issues such as the future end-users' anticipated fears and perceived benefits; (2) proposing a theoretical framework that tests the influence of various antecedent factors of behavioral intention to accept and further recommend biometric systems, gathered through a fresh integration of TAM, DOI theory and UTAUT along with the trust-privacy research field thus answering a call for a more integrative understanding of technology acceptance; (3) developing a model that is more focused and technology specific; (4) not limiting the framework to the often seen "intention to accept" variable but also expanding it to the behavioral intention to further recommend the use of biometrics; and (5) examining acceptance of biometric systems in voluntary settings thus providing important insight into the free formation of attitudes toward more radical technologies such as biometric systems. Further details on the contributions and the results are provided below.

A major academic contribution of our research is the theoretical framework presented in Fig. 1, which transcends the majority of previous TA formation models by looking at a more complete nature of the relationship between TA antecedents such as some of the famous theories' adoption variables, variables for the trust-privacy literature and behavioral intention to accept the new IT system.

Overall, the biometric system acceptance model proposed in this study is partially validated. Regarding the part of this model corresponding to TAM variables, although the influence of PU on BI (H1) is confirmed as in Kumar et al. [52] study to explain intention to use a firewall or in Gwebu and Wang [36] to explain intention to adopt open source software, both influences of PEOU on BI (H2) and on PU

(H3) are not validated. This reveals that for new technology, such as iris recognition, the perceived ease of use is not relevant to explain behavioral intention, such as in Zhou et al. [101] study on mobile banking. Perceived ease of use appears as an inhibitor of perceived usefulness which may suggest that young people can hardly understand the perceived ease of use of iris recognition. Stakeholders (e.g. managers, policy makers) should fully consider the importance to improve the perceived ease of use of this technology to achieve higher level of biometric systems acceptance. The influences of the DOI compatibility variable on PU (H4a), PEOU (H4b) and BI (H5) are also all validated and confirm the importance of this variable in technology acceptance models.

Regarding the UTAUT model, the influence of facilitating conditions on BI is confirmed (H7), whereas the impact of social influence (H6) is not validated. Similar result was obtained in [40,7]. It may mean that social influence is not as much relevant for this kind of technology as other variables in our model such as trust in technology, innovativeness, compatibility and perceived risks.

The results also confirm the direct effect of trust in technology on BI (H9d) but not the indirect influence through PU (H9b), PEOU (H9c) and perceived risks (H9a). This is consistent with findings from Chiu et al. [17] indicating that trust remains an important predictor of the repeated online buying intentions. That trust in technology is not relevant to explain perceived risks is counter intuitive however given the wealth of literature in this area [17,60]. One possible explanation is that although biometric systems are becoming more mature, users still lack solid enough knowledge about the technology and thus cannot completely realize the associated risks with it.

Both hypotheses about privacy and perceived risks are confirmed, i.e. the concern for data privacy has a direct effect on perceived risks (H10), and perceived risks have a direct effect on BI (H8). Both the concern for privacy and the perceived risks thus appear as relevant decision criteria to explain adoption of biometrics systems. It is necessary to guaranty that these two issues have been covered before launching a new biometric system into the market.

The innovativeness construct proved to have both a direct (H11d) and an indirect effect on BI through compatibility (H11c) but the indirect effects through both PEOU (H11b) and PU (H11a) are not validated. The direct and indirect effect of innovativeness on BI is in accordance with the findings from Agarwal and Prasad [2].

Finally, behavioral intention to accept biometrics explains 42% of the variation in recommendation (therefore validating H12). We can conclude this is an important contribution of our study because our model explains very well this concept and the recommendation power is rarely studied in the technology acceptance literature despite its huge interest [61].

There are two important conclusions driven by these results. First, that PEOU (H2) and social influence (H6) do not have the hypothesized influence on BI may be due to the fact that we have more variables in our model than in the isolated seminal theories from which these variables come from (i.e. TAM, DOI and UTAUT). The influence of these new variables turns out to be more important than that of the seminal variables, such as PEOU used in TAM or social influence from UTAUT. Second, that compatibility influences both PU and PEOU support the connection of DOI and TAM to explain technology acceptance. However, DOI seems much more appropriate than TAM to explain biometrics acceptance (both compatibility and innovativeness are confirmed here as influential factors) as only the influence of PU on BIA is confirmed as concerns the TAM model.

Our work thus contributes to existing literature pertaining to technology acceptance theories and complements existing models by providing an extended conceptual framework and new key determinants of technology adoption, such as perceived risks. We have included prior factors, such as trustworthiness, innovativeness, and concern for data privacy in our model that confirmed their either direct or indirect influence on BI and recommendation. We believe these variables should be utilized as valuable predictors of behavior in future work on technology adoption. In addition, this study extends TA theory by studying the potential recommendation power.

This paper offers additional contributions to its field of research. Although some previous studies have talked about biometric systems, few authors have assessed in detail how consumers react to biometrics, the antecedents of their perceptions, and the conditions under which some of these perceptions – in particular the perceived risks – can be prevailed over, e.g. in reducing the corresponding concerns for data privacy. Of course there have been a few exceptions to this (e.g. [83]) but we believe this is the most comprehensively empirical study up to this point. Our work maintains a focus on biometric systems end-users and contributes to the existing literature on identification technologies and privacy. What is more, our scenario-based approach allowed us to achieve a level of richness of empirical data which has previously not been possible in this field due to the novelty of the technology under investigation.

5.2. Practical implications

The use of biometric identification systems is growing in various industries (e.g. transportation, healthcare, grocery, financial sector) and government sectors [27]. Concurrently, a lack of understanding of the challenges and constraints in implementing biometrics has resulted in many organizations investing less or not investing at all in biometrics [10]. This study serves as an early attempt to empirically test the determinants of biometric identification systems acceptance. The results of this study provide useful and valuable information for all stakeholders (i.e. the personal identification service providers, governments, private enterprises…) that are contemplating to offer users this security feature in their everyday applications.

By exploring specific drivers (i.e. PU, PEOU) and inhibitors (i.e. risks) of biometric identification systems acceptance, this research offers opportunities to suppress the impact of inhibitors and promote acceptance enablers. The findings encourage practitioners to carefully consider the potential benefits and thoroughly evaluate risks associated with the implementation of this technology in a broader sense. This is important as some organizations and/or people might be attracted to adopt such technology due to its perceived usefulness but could ultimately refuse to implement it because of high perceived risks, especially in relation to security and privacy.

Globally, we have identified three main areas important to practice that significantly influence the intention to accept biometric identification systems. The first area is concerned with *specific characteristics of the potential target user* and encompasses factors, such as personal innovativeness, trust in technology, and concern for data privacy. Innovativeness is one of the adopter's characteristics that can assist biometric identification systems providers to first promote the technology to well-informed individuals. As such, they can identify the medium or area that is close to these individuals to promote biometric identification systems. For example, they can attract this target group via seminars, discussion groups or magazines focusing on this technology. With this, providers can run a more cost-efficient promo campaign with better chances of getting the segment market they are interested in. Next, the results suggest that identification service providers need to adopt differentiated approaches to build users' initial trust in biometric identification systems. When the target users have relatively high self-efficacy, such as young individuals, service providers need to present added-value services to them as these users mainly build their initial trust via the central route. On the other hand, when the target users have low self-efficacy, such as those that are unfamiliar with biometrics, service providers need to highlight ease of use and usefulness. In addition, while biometric user data is very sensible to

potential misuse, biometric identification systems should be set up with suitable security measures (e.g. encryption of collected personal data in the database and device/application supporting the identification process). Interestingly, our model hasn't revealed any relation between trust in biometric technologies and perceived risk and only confirmed the influence of concern for data privacy on risk. Such insight suggests that for a more radical technology the risks should be mitigated mostly by reducing people's concerns about privacy rather than through trust. This non-significant relationship between trust and risk was surprising because in other fields, for example in e-commerce, there is a strong relation between trust and risk perception. One explication for this result could be there are still rather few users who interact with this kind of technology in daily lives. Another reason could be that citizens perceive different identification technologies differently. Perhaps the perception of risk in e-commerce setting is more prevalent than in biometric identification settings. Or, perhaps there are different trust constructs that affect risk in biometric systems environments. Future research should address these potential differences.

The second area of practical implications deals with *antecedent factors of biometric systems acceptance* and comprises factors such as perceived ease of use, perceived usefulness, compatibility and perceived risks. Perceived ease of use is a biometric information system's characteristic that identification providers need to pay special attention to when offering the system to the user. Providers should aim at providing easy-to-use and intuitive identification devices that are simple to use (e.g. straightforward display, intuitive steps, guided help) and oriented to promptly solving potential problems users may encounter (e.g. guided tutorial assisting users in solving common errors arising from use). Next, the results also suggest perceived usefulness is another characteristic worth considering. Compared to other identification means biometric systems offer convenience in terms of user identification over traditional methods (e.g. by abolishing the need to remember passwords or PINs). In praxis this is particularly useful for those identification cases that are rarely used (e.g. library access, club member access, tax return filling system). Yet, although useful, organizations should still give their customers the option of using the normal security identification methods so as not to totally discourage them by imposing a system they might not be entirely comfortable with. Likewise, compatibility of biometric identification system with existing information systems is also an important characteristic for organizations to reflect on. Adoption of these systems entails the selection and implementation of different security standards between these systems and existing transactional systems (e.g. ERP system, CRM systems). The objective is to enhance the compatibility and flexibility of the overall organization's IT infrastructure. Whether or not biometric identification systems is perceived as better choice than the authentication currently used in an organization is closely related to the degree of perceived importance on standard compliance, interoperability, and interconnectivity. Since each organization is facing a different set of constraints (e.g. depending on the regulations and limitations of the industry they reside in), these aspects will hardly be identical. Lastly, our findings conform to findings of numerous studies (e.g. [42,43,65,69,70]) proposing risk as an important inhibitor to the acceptance of risky technologies. Identification service providers should find ways to reduce or mitigate risks and concerns of users when using biometric identification systems. These concerns can be mitigated by promoting reduced risks of security and identity fraud associated with biometrics use compared to traditional identification means, such as security cards, tokens, and passwords.

Last, but not least, *environmental factors*, such as facilitating conditions, are another important area with practical implications. The finding about positive relationship between facilitating conditions and intention to use biometric identification systems provides us an important perspective for practice. It sets out the path for organizations and governmental/regulatory sector to actively move for strengthening positive perceptions about biometric identification systems by developing targeting policies and regulations to govern the identification part of user authentication and to assure citizens about the reliability of these systems.

5.3. Limitations and suggestions for further research

This research has its own limitations that should encourage further research in this area. There are two major limitations of this study which we must draw attention to. First of all, our research focused only on one type of biometric system: iris scanning. Other types of biometrics of course carry their own advantages and disadvantages and it is possible that our results may have been marginally altered had a fingerprints or face recognition been considered by participants instead.

The second significant limitation of this paper concerns the age range of the sample. The respondents to this survey ranged between 15 years old and 25 years old, meaning that older demographics are unrepresented in this research. This is important as the older generations are sometimes portrayed as more suspicious of such invasive technologies and this may be an obstacle to the generalization of our results.

There are other limitations which could also form the basis for future work in this area to transcend the work conducted here. Notably, the conceptual framework should be tested on other samples (other European countries and non-European countries) and on samples as representative as possible of the whole population (not only 15–25 year olds) in order to see if all hypotheses postulated can be verified. Moreover, there are many exogenous factors that might influence responses which should be considered and explored in future research. Exogenous factors could include 'users' security perception on biometrics systems' (e.g. [54]), 'consumer traits' (e.g. [20]), 'situational factors' (e.g. [93]), 'product characteristics' (e.g. [28]), and 'previous experiences' (e.g. [25]). Additional research should thus investigate these other factors and their effect on consumer behavioral intention to accept new technologies in general and biometrics in particular.

We focused our research on young citizens' likelihood of acceptance of biometric systems, studying their reasons for accepting biometric electronic identification means. As a complementary view, it would also be interesting to study how (instead of why) they adopt such kinds of technologies, as the agency of the end-user does not end with the decision to adopt or reject the technology, but continues to actively shape how the technology is used, in what contexts and for what purposes, which may be rather different from the uses, contexts and purposes envisaged by the originators of the technology. In addition, it would also be appealing to examine the motivations of – public and private – organizations, their perceived risks in the implementation of biometrics, and the effects of private companies or public bodies in enabling this process (e.g. e-government initiatives such as e-passport).

Finally, whichever modeling approach is decided upon, researchers must acknowledge its inherent limitations. It has been noted that UTAUT itself fails to clearly define successful technology acceptance, or eliminate problems with the scaling of results. Venkatesh et al. [87] among others ([91]) have noted UTAUT's inability to adequately account for changes in intention. While our integrative model seeks to improve upon previous partial explanations of technology acceptance, it inevitably carries its own limitations. For example, measuring TAM and DOI using only some of the original variables is undoubtedly restrictive; other elements such as trialability and observability could also have significant effects, and might usefully be added to future models of existing technology acceptance, where their impacts could be more effectively measured than in our futuristic scenario.

Funding

This study was funded by the European Commission IPTS (Institute for Prospective Technological Studies) Joint Research Centre (EC JRC IPTS Contract No. 150876-2007 F1ED-FR).

The authors thank Ioannis Maghiros, Wainer Lusoli, and Margherita Bacigalupo from the European Commission IPTS Joint Research Centre for their support and confidence.

Appendix A. The biometric scenario tested in the research

Biometric scenario	eID technology	Application
Your friend *Alex* is 17. Every day he goes to the library to practice for his driving test on one of the driving simulators provided by the local council. To enter the library he could join the queue at the counter, which is half-dozen people long, including people he knows, and have his library card scanned. The librarian will look at his file, ask him a few questions and allocate the right simulator. Alternatively, he could use the eye-scan machine at the entrance. This automatically allocates him a simulator to use, based on his previous test results and on his preferences. The second procedure will probably take less time.	Biometrics (iris recognition)	Facilitating person-bound (non-remote) services

Appendix B. Main characteristics of the sample (demographics and internet use)

Demographic characteristics (%)			Internet use (%)		
Sex	Male	67%	Internet connection type	Broadband at home	91%
	Female	33%		Other connections	9%
Age	15–18	26.5%	Internet length of use	<1 year	3%
	19–21	42%		1–3 years	6%
	22–25	31.5%		3–5 years	14%
Professional status	Student	27%		+5 years	77%
	Self-employed	9.5%	Surf online	Several times per day	80%
				Once a day	14
	Manager	17%		Once a day	14%
	Other white collar	10%		A few times a week	4%
	Blue collar	4%		Less than once a week	2%
	Unemployed	10%			

Appendix C. Instruments measure

Variable	Sample question*	Source
Perceived usefulness (PU)	This system would make it easier to identify oneself	Davis [21]
Perceived ease of use (PEOU)	Learning to use such service would be easy for me	Davis [21]
Compatibility (COMP)	Using this system would fit into my lifestyle	Vijayasarathy [89]
Facilitation conditions (FC)	If the service is free	Self-developed from literature
Perceived risks (PR)	Someone may hack into the system and steal your personal information	Bélanger and Carter [5]
Trust in technology (TT)	I would trust the system	Pavlou [69]
Privacy concerns (PC)	I am concerned that my personal data is shared with third parties without my agreement	Fogel and Nehmad [29]
Innovativeness (I)	I like to experiment with new technologies	Yi et al. [98]
Intention of eID acceptance (BI)	I should apply this service as soon as possible	Self-developed from literature
Recommendation (REC)	Would you recommend that your friends subscribe to the service?	Self-developed from literature

*The whole list of items is available upon request to the first author.

Appendix D. Total and direct effects

Path	Total effect (direct effect)	Total t-stat (direct t-stat.)
Behavioral intention (BI)		
PU → BI	0.202^{***} (0.202^{***})	4.296 (4.192)
PEOU → BI	−0.033 (0.005)	0.496 (0.084)
Compatibility → BI	0.237^{***} (0.145^{*})	2.908 (1.765)
SI → BI	0.061 (0.061)	1.297 (1.303)
FC → BI	0.103^{**} (0.103^{**})	2.437 (2.338)
PR → BI	-0.106^{**} (-0.106^{**})	2.217 (2.122)
Trust TECH → BI	0.249^{***} (0.246^{***})	3.311 (3.318)
Innovativeness → BI	0.255^{***} (0.208^{***})	4.934 (4.098)
PC → BI	-0.036^{*}	1.960
Perceived usefulness (PU)		
PEOU → PU	-0.190^{**} (-0.190^{**})	2.380 (2.298)
Compatibility → PU	0.440^{***} (0.529^{***})	5.691 (5.837)
Trust TECH → PU	−0.025 (−0.007)	0.315 (0.089)
Innovativeness → PU	0.053 (−0.031)	1.043 (0.616)
Perceived ease of use (PEOU)		
Compatibility → PEOU	0.469^{***} (0.469^{***})	5.631 (5.939)
Trust TECH → PEOU	0.094 (0.094)	1.150 (1.166)
Innovativeness → PEOU	0.219^{***} (0.108^{**})	3.767 (2.184)
Perceived risks (PR)		
Trust TECH → PR	−0.071 (−0.071)	1.153 (1.155)
PC → PR	0.338^{***} (0.338^{***})	6.090 (5.862)
Compatibility (Comp)		
Innovativeness → Compatibility	0.239^{***} (0.239^{***})	4.501 (4.592)
Recommendation (REC)		
BI → Recommend	0.648^{***} (0.648^{***})	18.451 (18.467)
PU → Recommend	0.131^{***}	4.107
PEOU → Recommend	−0.021	0.497
Compatibility → Recommend	0.153^{**}	2.883
SI → Recommend	0.040	1.288
FC → Recommend	0.067^{**}	2.402
PR → Recommend	-0.068^{**}	2.199
Trust TECH → Recommend	0.161^{***}	3.239
PC → Recommend	-0.023^{*}	1.941
Innovativeness → Recommend	0.165^{***}	4.952

Note: $^{*}p < 0.10$; $^{**}p < 0.05$; $^{***}p < 0.01$; the constructs are standardized (mean 0 and standard deviation 1).

References

[1] M.G. Aboelmaged, Predicting e-procurement adoption in a developing country: an empirical integration of technology acceptance model and theory of planned behaviour, Industrial Management & Data Systems 110 (3) (2010) 392–414.
[2] R. Agarwal, J. Prasad, A conceptual and operational definition of personal innovativeness in the domain of information technology, Information Systems Research 9 (2) (1998) 204–215.
[3] E.W. Baker, S.S. Al-Gahtani, G.S. Hubona, Cultural impacts on acceptance and adoption of information technology in a developing country, Journal of Global Information Management 18 (3) (2010) 35–58.
[4] B.A. Beemer, D.G. Gregg, Dynamic interaction in knowledge based systems: an exploratory investigation and empirical evaluation, Decision Support Systems 49 (4) (2010) 386–395.
[5] F. Bélanger, L. Carter, Trust and risk in e-government adoption, The Journal of Strategic Information Systems 17 (2) (2008) 165–176.
[6] J. Benamati, M.A. Fuller, M.A. Serva, J. Baroudi, Clarifying the integration of trust and TAM in E-commerce environments: implications for systems design and management, IEEE Transactions on Engineering Management 57 (3) (2010) 380–393.
[7] A. Bhattacherjee, J. Perlos, C. Sanford, Information technology continuance: a theoretical extension and empirical test, The Journal of Computer Information Systems 49 (1) (2008) 17–26.
[8] E. Bigné-Alcañiz, C. Ruiz-Mafé, J. Aldás-Manzano, S. Sanz-Blas, Influence of online shopping information dependency and innovativeness on internet shopping adoption, Online Information Review 32 (5) (2008) 648–667.
[9] L. Carter, F. Bélanger, The utilization of e-government services: citizen trust, innovation and acceptance factors, Information Systems Journal 15 (1) (2005) 5–25.
[10] A. Chandra, T. Calderon, Challenges and constraints to the diffusion of biometrics in information systems, Communications of the ACM 48 (12) (2005) 101–106.
[11] C.-D. Chen, Y.-W. Fan, C.-K. Farn, Predicting electronic toll collection service adoption: an integration of the technology acceptance model and the theory of planned behavior, Transportation Research Part C: Emerging Technologies 15 (5) (2007) 300–311.

[12] Y.H. Cheng, Y.J. Yeh, Exploring radio frequency identification technology's application in international distribution centers and adoption rate forecasting, Technological Forecasting and Social Change 78 (4) (2011) 661–673.
[13] T.C.E. Cheng, D.Y.C. Lam, A.C.L. Yeung, Adoption of internet banking: an empirical study in Hong Kong, Decision Support Systems 42 (3) (2006) 1558–1572.
[14] W.W. Chin, Issues and opinion on structural equation modeling, MIS Quarterly 22 (1) (1998) VII–XVI.
[15] W.W. Chin, B.L. Marcolin, P.R. Newsted, A partial least squares latent variable modeling approach for measuring interaction effects: results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study, Information Systems Research 14 (2) (2003) 189–217.
[16] C.-M. Chiu, E.T.G. Wang, Understanding web-based learning continuance intention: the role of subjective task value, Information Management 45 (3) (2008) 194–201.
[17] C.-M. Chiu, H.-Y. Huang, C.-H. Yen, Antecedents of trust in online auctions, Electronic Commerce Research and Applications 9 (2) (2010) 148–159.
[18] H. Cho, M. Rivera-Sánchez, S. Sun Lim, A multinational study on online privacy: global concerns and local responses, New Media & Society 11 (3) (2009) 395–416.
[19] R. Clodfelter, Biometric technology in retailing: will consumers accept fingerprint authentication? Journal of Retailing and Consumer Services 17 (3) (2010) 181–188.
[20] P.A. Dabholkar, R.P. Bagozzi, An attitudinal model of technology-based self-service: moderating effects of consumer traits and situational factors, Journal of the Academy of Marketing Science 30 (3) (2002) 184–201.
[21] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly (1989) 319–340.
[22] F. Deane, K. Barrelle, R. Henderson, D. Mahar, Perceived acceptability of biometric security systems, Computer Security 14 (3) (1995) 225–231.
[23] M.T. Dishaw, D.M. Strong, Extending the technology acceptance model with task–technology fit constructs, Information Management 36 (1) (1999) 9–21.
[24] S. Djamasbi, D.M. Strong, M. Dishaw, Affect and acceptance: examining the effects of positive mood on the technology acceptance model, Decision Support Systems 48 (2) (2010) 383–394.
[25] M.A. Eastlick, S. Lotz, Profiling potential adopters and non-adopters of an interactive electronic shopping medium, International Journal of Retail & Distribution Management 27 (6) (1999) 209–223.
[26] E.M. Eisenstein, Identity theft: an exploratory study with implications for marketers, Journal of Business Research 61 (11) (2008) 1160–1172.
[27] W. Elgarah, N. Falaleeva, Adoption of biometric technology: information privacy and TAM, Proceedings of the Eleventh Americas Conference on Information Systems, 2005.
[28] S. Elliot, S. Fowell, Expectations versus reality: a snapshot of consumer experiences with internet retailing, International Journal of Information Management 20 (2000) 323–336.
[29] J. Fogel, E. Nehmad, Internet social network communities: risk taking, trust, and privacy concerns, Computers in Human Behavior 25 (1) (2009) 153–160.
[30] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, Journal of Marketing Research 18 (1) (1981) 39–50.
[31] D. Gefen, D.W. Straub, The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption, Journal of the Association for Information Systems 1 (1) (2000) 1–28.
[32] D. Gefen, D. Straub, Managing user trust in B2C e-services, e-Service Journal 2 (2) (2003) 7–23.
[33] D. Gefen, D.W. Straub, Consumer trust in B2C e-commerce and the importance of social presence: experiments in e-products and e-services, Omega 32 (6) (2004) 407–424.
[34] R. Goldsmith, L.R. Flynn, Identifying innovators in consumer product markets, European Journal of Marketing 26 (12) (1992) 42–55.
[35] J. Grijpink, An assessment model for the use of biometrics, Computer Law & Security Review 22 (4) (2006) 316–319.
[36] K.L. Gwebu, J. Wang, Adoption of open source software: the role of social identification, Decision Support Systems 51 (1) (2011) 220–229.
[37] S. Ha, L. Stoel, Consumer e-shopping acceptance: antecedents in a technology acceptance model, Journal of Business Research 62 (5) (2009) 565–571.
[38] J.D. Hartog, R.V. Munster, Biometrics at the turnstiles, Computer Weekly 156 (2008) 20–22.
[39] C.-L. Hsu, H.-P. Lu, Why do people play on-line games? An extended TAM with social influences and flow experience, Information Management 41 (7) (2004) 853–868.
[40] S.-Y. Hung, C.-M. Chang, T.-J. Yu, Determinants of user acceptance of the e-Government services: the case of online tax filing and payment system, Government Information Quarterly 23 (1) (2006) 97–122.
[41] I. Im, S. Hong, M.S. Kang, An international comparison of technology adoption: testing the UTAUT model, Information Management 48 (1) (2011) 1–8.
[42] S.L. Jarvenpaa, D.E. Leidner, Communication and trust in global virtual teams, Organization Science 10 (6) (1999) 791–815.
[43] S.L. Jarvenpaa, N. Tractinsky, M. Vitale, Consumer trust in an internet store, Information Technology and Management 1 (12) (2000) 45–71.
[44] L.A. Jones, A.I. Ant, J.B. Earp, Towards understanding user perceptions of authentication technologies, Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, ACM, Alexandria, Virginia, USA, 2007, pp. 91–98.
[45] S. Kim, J.Y. Son, Out of dedication or constraint? A dual model of post-adoption phenomena and its empirical test in the context of online services, MIS Quarterly 32 (4) (2009) 49–70.
[46] H.W. Kim, H.C. Chan, S. Gupta, Value-based adoption of mobile internet: an empirical investigation, Decision Support Systems 43 (1) (2007) 111–126.
[47] D.J. Kim, D.L. Ferrin, H.R. Rao, A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents, Decision Support Systems 44 (2) (2008) 544–564.
[48] C. Kim, M. Mirusmonov, I. Lee, An empirical examination of factors influencing the intention to use mobile payment, Computers in Human Behavior 26 (3) (2010) 310–322.
[49] N. Koenig-Lewis, A. Palmer, A. Moll, Predicting young consumers' take up of mobile banking services, International Journal of Bank Marketing 28 (5) (2010) 410–432.
[50] S.Y.X. Komiak, I. Benbasat, The effects of personalization and familiarity on trust and adoption of recommendation agents, MIS Quarterly 30 (4) (2006) 941–960.
[51] M. Koufaris, W. Hampton-Sosa, The development of initial trust in an online company by new customers, Information Management 41 (3) (2004) 377–397.
[52] N. Kumar, K. Mohan, R. Holowczak, Locking the door but leaving the computer vulnerable: factors inhibiting home users' adoption of software firewalls, Decision Support Systems 46 (1) (2008) 254–264.
[53] Y.-F. Kuo, S.-N. Yen, Towards an understanding of the behavioral intention to use 3G mobile value-added services, Computers in Human Behavior 25 (1) (2009) 103–110.
[54] D. Laux, A. Luse, B. Mennecke, A.M. Townsend, Adoption of biometric authentication systems: implications for research and practice in the deployment of end-user security systems, Journal of Organizational Computing and Electronic Commerce 21 (3) (2011) 221–245.
[55] M.-C. Lee, Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and perceived benefit, Electronic Commerce Research and Applications 8 (3) (2009) 130–141.
[56] M.C. Lee, Predicting and explaining the adoption of online trading: an empirical study in Taiwan, Decision Support Systems 47 (2) (2009) 133–142.
[57] K. Lee, A. Yan, K. Joshi, Understanding the dynamics of users' belief in software application adoption, International Journal of Information Management 31 (2) (2011) 160–170.
[58] C. López-Nicolás, F.J. Molina-Castillo, H. Bouwman, An assessment of advanced mobile services acceptance: contributions from TAM and diffusion theory models, Information Management 45 (6) (2008) 359–364.
[59] P. Lucas, Biometrics come into focus, American Banker 10 (3) (2005) 18–21.
[60] X. Luo, H. Li, J. Zhang, J.P. Shim, Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: an empirical study of mobile banking services, Decision Support Systems 49 (2) (2010) 222–234.
[61] W.W. Moe, D.A. Schweidel, Online product opinions: incidence, evaluation, and evolution, Marketing Science 31 (3) (2012) 372–386.
[62] G.C. Moore, I. Benbasat, Development of an instrument to measure the perceptions of adopting an information technology innovation, Information Systems Research 2 (3) (1991) 192–222.
[63] C. Morosan, Theoretical and empirical considerations of guests' perceptions of biometric systems in hotels: extending the technology acceptance model, Journal of Hospitality and Tourism Research 36 (1) (2012) 52–84.
[64] G. Ng-Kruelle, P.A. Swatman, J.F. Hampe, D.S. Rebne, Biometrics and e-identity (e-passport) in the European Union: end-user perspectives on the adoption of a controversial innovation, Journal of Theoretical and Applied Electronic Commerce Research 1 (2) (2006) 12–35.
[65] P.A. Norberg, D.R. Horne, D.A. Horne, The privacy paradox: personal information disclosure intentions versus behaviors, Journal of Consumer Affairs 41 (1) (2007) 100–126.
[66] J.C. Nunnally, Psychometric Theory, McGraw-Hill, New York, 1978.
[67] O. O'Neill, A Question of Trust, Cambridge University Press, Madrid, Spain, 2002.
[68] W.J. Orlikowski, C.S. Iacono, Research commentary: desperately seeking the "IT" in IT research — a call to theorizing the IT artifact, Information Systems Research 12 (2) (2001) 121–134.
[69] P.A. Pavlou, Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model, International Journal of Electronic Commerce 7 (3) (2003) 101–134.
[70] P.A. Pavlou, D. Gefen, Building effective online marketplaces with institution-based trust, Information Systems Research 15 (1) (2004) 37–59.
[71] A.P. Pons, P. Polak, Understanding user perspectives on biometric technology, Communications of the ACM 51 (9) (2008) 115–118.
[72] N.J. Rifon, R. LaRose, S.M. Choi, Your privacy is sealed: effects of web privacy seals on trust and personal disclosures, Journal of Consumer Affairs 39 (2) (2005) 339–362.
[73] J.C. Roca, J.J.G. Machado, J.J.D.L. Vega, Personal innovativeness, security and privacy as determinants of e-trading adoption, International Journal of Electronic Finance 4 (3) (2010) 269–286.
[74] E.M. Rogers, Diffusion of Innovations, 5th edition Free Press, New York, 2003.
[75] M. Scott, T. Acton, M. Hughes, An assessment of biometric identities as a standard for e-government services, International Journal of Services and Standards 1 (3) (2005) 271–286.
[76] P.B. Seddon, A respecification and extension of the DeLone and McLean model of IS success, Information Systems Research 8 (3) (1997) 240–253.
[77] S.A. Shaikh, J.R. Rabaiotti, Characteristic trade-offs in designing large-scale biometric-based identity management systems, Journal of Network and Computer Applications 33 (3) (2010) 342–351.
[78] C.-C. Shen, J.-S. Chiou, The impact of perceived ease of use on internet service adoption: the moderating effects of temporal distance and perceived risk, Computers in Human Behavior 26 (1) (2010) 42–50.

[79] A. Srivastava, Electronic signatures and security issues: an empirical study, Computer Law & Security Review 25 (5) (2009) 432–446.
[80] A. Taneja, A. Wang, M.K. Raja, Assessing the impact of concern for privacy and innovation characteristics in the adoption of biometric technologies, 37th Annual Conference of Decision Sciences Institute, Decision Sciences Institute, Bricktown-Oklahoma City, 2006.
[81] F. Thiesse, RFID, privacy and the perception of risk: a strategic framework, The Journal of Strategic Information Systems 16 (2) (2007) 214–232.
[82] U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain, Biometric cryptosystems: issues and challenges, Proceedings of the IEEE 92 (6) (2004) 948–960.
[83] F.-M.E. Uzoka, Fuzzy-expert system for cost benefit analysis of enterprise information systems: a framework, International Journal on Computer Science and Engineering 1 (3) (2009) 254–262.
[84] V. Venkatesh, H. Bala, Technology acceptance model 3 and a research agenda on interventions, Decision Sciences 39 (2) (2008) 273–315.
[85] V. Venkatesh, S.A. Brown, A longitudinal investigation of personal computers in homes: adoption determinants and emerging challenges, MIS Quarterly (2001) 71–102.
[86] V. Venkatesh, F.D. Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, Management Science (2000) 186–204.
[87] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: toward a unified view, MIS Quarterly (2003) 425–478.
[88] V. Venkatesh, J.Y.L. Thong, X. Xu, Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology, MIS Quarterly 36 (1) (2012) 157–178.
[89] L.R. Vijayasarathy, Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model, Information Management 41 (6) (2004) 747–762.
[90] Y.-S. Wang, Y.-W. Liao, Assessing eGovernment systems success: a validation of the DeLone and McLean model of information systems success, Government Information Quarterly 25 (4) (2008) 717–733.
[91] P.R. Warshaw, F.D. Davis, Disentangling behavioral intention and behavioral expectation, Journal of Experimental Social Psychology 21 (3) (1985) 213–228.
[92] D. Wolfe, User milestone for a biometric system, American Banker 173 (190) (2008).
[93] M. Wolfinbarger, M.C. Gilly, Shopping online for freedom, control, and fun, California Management Review 43 (2) (2001), (34–+).
[94] I.-L. Wu, J.-L. Chen, An extension of Trust and TAM model with TPB in the initial adoption of on-line tax: an empirical study, International Journal of Human Computer Studies 62 (6) (2005) 784–808.
[95] J.M. Wu, A. Lederer, A meta-analysis of the role of environment-based voluntariness in information technology acceptance, MIS Quarterly 33 (2) (2009) 419–432.
[96] J.-H. Wu, S.-C. Wang, What drives mobile commerce?: an empirical evaluation of the revised technology acceptance model, Information Management 42 (5) (2005) 719–729.
[97] I.L. Wu, J.Y. Li, C.Y. Fu, The adoption of mobile healthcare by hospital's professionals: an integrative perspective, Decision Support Systems 51 (3) (2011) 587–596.
[98] M.Y. Yi, J.D. Jackson, J.S. Park, J.C. Probst, Understanding information technology acceptance by individual professionals: toward an integrative view, Information Management 43 (3) (2006) 350–363.
[99] S.Y. Yousafzai, G.R. Foxall, J.G. Pallister, Explaining internet banking behavior: theory of reasoned action, theory of planned behavior, or technology acceptance model? Journal of Applied Social Psychology 40 (5) (2010) 1172–1202.
[100] C.S. Yu, Factors affecting individuals to adopt mobile banking: empirical evidence from the UTAUT model, Journal of Electronic Commerce Research 13 (2) (2012) 104–121.
[101] T. Zhou, Y. Lu, B. Wang, Integrating TTF and UTAUT to explain mobile banking user adoption, Computers in Human Behavior 26 (4) (2010) 760–767.
[102] J.C. Zimmer, R.E. Arsal, M. Al-Marzouq, V. Grover, Investigating online information disclosure: effects of information relevance, trust and risk, Information Management 47 (2) (2010) 115–123.

Dr. Caroline Lancelot Miltgen is an Associate Professor of Marketing at the University of Angers, France. She holds a Ph.D. in Management from the University of Paris Dauphine, France. Her current research interests include information privacy, e-commerce and public policy, social media and digital services, technology adoption and product innovation. She is the (co)author of papers in national and international scientific journals in Information Systems and Marketing. She was the principal investigator of two research contracts funded by the European Commission — 'Privacy and electronic identification systems' (2007) and 'Privacy and personal information data management' (2009).

Dr. Aleš Popovič is an Assistant Professor of Information Management at the Faculty of Economics at the University of Ljubljana and visiting professor at ISEGI — University Nova in Lisbon. He holds BS, MSC and Ph.D. degrees from the University of Ljubljana. His research focuses on business intelligence, information management, and business process management. He is the (co)author of numerous papers in national and international professional and scientific journals. He has collaborated in many applied projects in the areas of business process modeling, analysis, renovation and informatization and in the area of business intelligence.

Tiago Oliveira is an Invited Assistant Professor at the Instituto Superior de Estatística e Gestão de Informação of the Universidade Nova de Lisboa (ISEGI-UNL). He holds a Ph.D. from the Universidade Nova de Lisboa in Information Management. His research interests include technology adoption, digital divide and privacy. He has published papers in several academic journals and conferences, including the Information & Management, Journal of Global Information Management, Industrial Management & Data Systems, Applied Economics Letters, Electronic Journal of Information Systems Evaluation, Communications in Statistics — Simulation and Computation, and American Journal of Mathematical and Management Sciences among others. Additional detail can be found in, http://www.isegi.unl.pt/toliveira/.