Information & Management 52 (2015) 741–759

Contents lists available at ScienceDirect

Information & Management

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

Exploring information privacy regulation, risks, trust, and behavior

Caroline Lancelot Miltgen [a,*], H. Jeff Smith [b,1]

[a] Audencia School of Management, 8 route de la Jonelière, BP 31222, 44312 Nantes Cedex 3, France
[b] Department of Information Systems and Analytics, Farmer School of Business, Miami University, Oxford, OH, USA

ARTICLE INFO

Article history:
Received 20 August 2013
Received in revised form 5 May 2015
Accepted 4 June 2015
Available online 25 June 2015

Keywords:
Information privacy
Protection
Regulation
Trust
Risk
Rewards

ABSTRACT

Over the past few decades, governments worldwide have grappled with their approaches to regulating issues associated with information privacy. However, research on individuals' perceptions of regulatory protections and the relationships between those perceptions and behavioral choices has been sparse.

In this study, we develop and test a model that considers relationships between an antecedent variable (regulatory knowledge); a mediating structure that encompasses perceived privacy regulatory protection, trust, and privacy risk concerns; two outcome variables (protection behavior and regulatory preferences); and direct and moderating effects of perceived rewards. Using a sample of young UK consumers that we collected in cooperation with the European Commission, we find strong support for our overall model and for most of our hypotheses.

We discuss implications for research, managerial practice, and regulation.

1. Introduction

Beginning in the 1970s, worldwide attention has been focused on information privacy. By 1986, privacy had been denoted as one of the four "ethical issues of the information age" [46]. As the years have passed, concerns about information privacy have only increased. A 2008 poll found that "72 percent of consumers are concerned that their online behavior [is] being tracked and profiled by companies" [18]. In a spring 2011 survey, 98 percent of 1000 smartphone users indicated that privacy was an important concern when using a mobile device, and over one-third of them (38%) identified privacy as their top concern [32]. It is clear that consumers are worried about privacy.

Over this same time frame—from the 1970s to today—governments around the world have grappled with their approaches to regulating issues associated with information privacy. Their approaches have differed greatly, however [27,49,69], and it is apparent that varying regulatory approaches to cross-border data flows are causing great consternation among firms that compete internationally (e.g., [39,68]). Examples of the tension abound. For example, in mid-2014, the European Court of Justice ruled that Google must erase links to certain content about individuals on the web when those individuals request this action [66], a ruling that many legal observers believe will have significant implications for many other firms that do business in Europe [78]. Ironically, it appears that consumer concerns associated with surveillance, reported extensively during 2013 and 2014 (see synthesis in [29]), are being directed more at commercial than governmental data interchanges [44].

One tacit assumption on the part of governmental regulators seems to be that regulations impact behavior. Ironically, in spite of the spike in international regulatory attention that is devoted to privacy issues and the tensions associated with them, there has been very little research on that relationship at either a corporate or an individual level. At the corporate level, one must look back nearly two decades to find a few studies (e.g., [70,73]). At the individual level, as will be discussed in the next section, there have been eight studies to date, but none of those studies have considered a comprehensive model that addresses the complexity of individuals' decision making.

Therefore, in this paper, we describe a study that explores new and richer relationships than those studied in the previous works in this area. Using a sample of young U.K. consumers that was gathered in cooperation with the European Commission, we test this model and find strong support for most of our hypotheses.

This study makes three important contributions to the literature.

First, the study is the first to construct a consolidated model that addresses a number of constructs related to governmental regulations and outcomes that had only been considered

* Corresponding author. Tel.: +33 240 378 141.
E-mail addresses: clancelot@audencia.com (C.L. Miltgen), jeff.smith@MiamiOH.edu (H.J. Smith).
[1] Tel.: +1 513 529 2093.

http://dx.doi.org/10.1016/j.im.2015.06.006
0378-7206/

separately in previous studies. Those earlier works had independently identified some variables and relationships that may explain a number of perceptions, attitudes, and behavior associated with privacy regulation. In this study, we extend these works by identifying the common components in their analyses.

Second, this paper provides empirical justification for relationships between several constructs that had heretofore been untested. We test a model that considers relationships between an antecedent variable (regulatory knowledge); a mediating structure that encompasses perceived privacy regulation protection, trust, and privacy risk concerns; two outcome variables (protection behavior and regulatory preferences); and direct and moderating effects of perceived rewards. This study is the first to look across that spectrum of relationships by considering some selected variables within each domain associated with privacy regulation.

Third, this study provides a starting set of measurement scales that can be used by future researchers as they delve more deeply into four constructs that had been given only limited attention in prior research—regulatory knowledge, privacy risk concerns, regulatory preferences, and perceived rewards—and their relationships.

This paper proceeds as follows. First, we provide background for the study by considering previous research. Then, we develop our own research model and detail the hypotheses of this model. Next, we discuss the study's method and detail our findings. We then discuss implications of this study not only for researchers but also for management and regulation.

2. Background

Our review of previous research in this domain reveals only eight studies that have examined, at the individual level, perceptions of or preferences for governmental privacy regulations (as either an independent or dependent variable) and their association with various constructs (perceptual and/or behavioral). Table 1 details these eight studies.

These studies have provided some insight into this phenomenon. A number of important antecedents have been considered. For example, cultural values [49,51], previous experiences [58], and awareness of laws [25] have been included in some studies. The manner in which regulatory attributes result in actions taken by individuals [25,45,82] and in the determination of regulatory preferences have also been explored in some papers [40,49]. Additionally, several mediating and moderating variables have been included in various studies. For example, demographic variables such as age, gender, and occupation [25,40,79,85] and individual attitudinal measures such as online privacy concerns [45,82] have been incorporated into some models. Thus, some forward movement has been observed in the research stream; at the same time, however, it is clear that these studies have not coalesced into a body of knowledge that can provide guidance to researchers, practitioners, managers, and regulators.

Therefore, to take one step toward a more cohesive knowledge base, we consider a model that looks across the "APCO" (antecedents–privacy concerns–outcomes) framework proposed by Smith et al. [71] by including constructs inspired by some of the previous studies in Table 1 (regulatory knowledge, perceived privacy regulatory protection, privacy risk concerns, protection behavior, and regulatory preferences), a construct that has been considered frequently in the broader privacy domain but that has heretofore been overlooked in studies on regulation (trust), and a construct (perceived rewards) that other privacy-related research studies have shown to be of some importance for individuals' decision making (e.g., [1,23,86]) but that has also been overlooked in regulation studies. Our objectives in testing this model are to provide a more cohesive view of privacy regulation findings and to extend those findings by incorporating what we believe to be some

Table 1
Previous studies—governmental regulation and outcomes (individual level).[a]

Article	Sample	Antecedents[b]	Dependent variable	Mediators/moderators
Dommeyer and Gross [25]	137 respondents to a mailed survey; list generated by broker	Awareness of privacy-related laws and privacy-protecting strategies	Use of privacy-protecting strategies (self-reported)	Age, gender, telephone number listing status, desire to receive direct marketing solicitations
Lee [40]	23 adults (selection procedure unclear)	Advocacy level	Desire for online regulation	Age, occupation
Lwin et al. [45]	180 adults provided by commercial research firm (experimental treatments applied)	Perceived influences (policy, regulation)	User intentions (self-reported)	Data sensitivity, data congruency, online privacy concern
Milberg et al. [49]	595 members of Information Systems Audit & Control Association at 63 chapter meetings	Cultural values	Privacy concerns, regulatory approach, corporate privacy management, privacy problems	Regulatory preference
Okazaki et al. [58]	510 mobile phone users, recruited by a professional research firm (experimental treatment applied)	Prior negative experience	Information privacy concerns, trust, risk, sensitivity of information request, perceived ubiquity	Preference for degree of regulatory control
Turow et al. [79]	1500 adults in a telephone survey (random dial sample)	None	Level of knowledge of privacy rules	Gender, age, race/ethnicity, education, family income, parental status
Wirtz et al. [82]	182 online subjects (recruited from commercial database)	Business policy, governmental regulation	User intentions (self-reported)	Privacy concerns
Xu et al. [85]	178 online web respondents (experimental treatments applied)	Individual self-protection, industry self-regulation, government legislation	Context-specific concerns for information privacy	Perceived control over personal information, age, gender, education, desire for information control, trust propensity, privacy experience

[a] Our search for articles was conducted using several online databases of scholarly articles. We began by searching salient keywords and proceeded by following citation trails that showed which articles were being cited by others. While we cannot claim that this list is fully exhaustive, we believe that it is largely comprehensive within the boundaries of our search algorithm.

[b] Antecedents, dependent variables, and mediators/moderators were categorized by this study's authors based on their reading of the cited articles.

of the most promising constructs from the broader privacy research domain. We now turn to the specific model that is addressed in this study.

3. Model development

As shown in Fig. 1 and Table 2, we examine the relationship between an antecedent (regulatory knowledge), a set of mediating variables (perceived privacy regulatory protection, trust, and privacy risk concerns), a set of outcomes (regulatory preferences and protection behavior), and a variable with both direct and moderating effects (perceived rewards). Our derivation of hypotheses relies on some of the articles listed in Table 1 and other studies that have examined subordinate portions of the model (even if they have not considered the regulatory constructs) or that have provided useful theoretical insights that may extrapolate to the immediate model. In addition, in some cases, we rely on our own argumentation to defend hypotheses. We do not claim that our model is exhaustive given the paucity of theoretical development in this research domain (see Table 1) and the constraints associated with data collection. Rather, we attempt to address a set of variables that is most likely to produce insights from this exploratory study and to inform future efforts in this domain.

3.1. Regulatory knowledge and perceived privacy regulatory protection

Smith et al. [71] noted that a small stream of research has focused on individuals' awareness of privacy policies and practices and how such awareness is associated with those individuals' perceptions and behavior. However, most of the studies in this category (e.g., [19,56,57]) focused on *organizational* policies and practices. It has been rare for researchers to consider relationships between individuals' level of knowledge regarding privacy *regulation* and other variables; to the best of our knowledge, only Dommeyer and Gross [25] took this approach.

Perceived privacy regulatory protection refers to an individual's perceptions regarding the existence and adequacy of provisions and systems for protecting his/her personal data. As will be discussed below (in Section 3.2), we view individuals' perceptions regarding privacy regulatory protection as a salient factor in determining their trust in entities associated with information privacy. It stands to reason that an individual's level of knowledge regarding such protection should factor into his or her perceptions of the protection itself. Ironically, however, past research (e.g., [49]) has not considered this relationship when assessing privacy regulation perceptions.

Given the paucity of previous research regarding this relationship, we are forced to form an exploratory hypothesis. We conjecture that many perceptions of inadequate regulatory protection may in fact be grounded in individuals' lack of knowledge regarding the protection that already exists. As was shown by Dommeyer and Gross [25], this level of knowledge is alarmingly low in some areas, and while we are unable to infer strict causality in this relationship, findings that consumers perceive regulation as lacking (e.g., [26]) are at least temporally correlated with this lack of knowledge. We state our hypothesis in the positive form, as follows:

H1. Higher levels of knowledge regarding regulation will be associated with higher levels of perceived privacy regulatory protection.

3.2. Trust

As was discussed by Smith et al. [71], the construct of trust has been considered in a number of research models of privacy. However, its specific relationship with other privacy-related constructs has not been consistently examined across studies, with trust serving as an antecedent, outcome, mediator, or moderator. In this study, for reasons that we will discuss below, we consider trust to have a mediating role.

To a great degree, our view of trust as a mediating construct is a function of the specific form of trust that is examined in our study: trust in governmental and commercial entities that are associated with information privacy. Note that this differs from interpersonal or dyadic trust, which is trust between *people*, whose relationships may or may not rest in an organizational domain [47,67]. The concept of trust that is considered in our study has been called "impersonal trust" [20]; it was explored by McKnight et al. [48] and considered in a complex research model by Bansal et al. [5].

To the best of our knowledge, prior research has not considered how impersonal trust (in both governmental and commercial entities) is associated with individuals' perceptions of regulatory protection. Although it may at first glance appear that such a relationship borders on the tautological (i.e., if one believes that one is safe in dealing with an entity, one will trust that entity), the demarcation considered in this study is more complex: individuals can have a high level of trust in their government and/or a commercial entity regardless of whether their own government

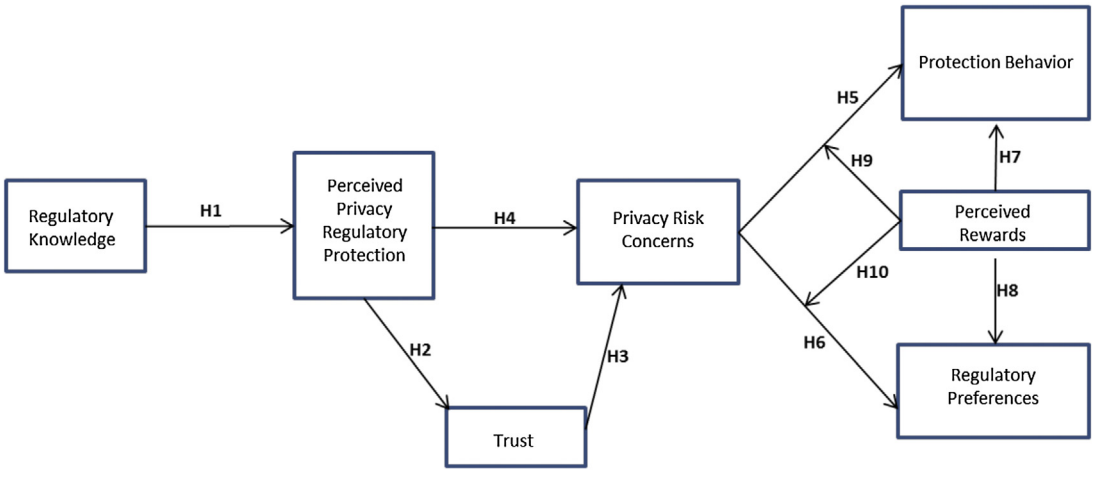

Fig. 1. Research model.

Table 2
Hypotheses.

H1	Higher levels of knowledge regarding regulation will be associated with higher levels of perceived privacy regulatory protection.
H2	Higher levels of perceived privacy regulatory protection will be associated with higher levels of trust in entities associated with information privacy.
H3	Higher levels of trust in entities associated with information privacy will be associated with lower levels of privacy risk concerns.
H4	Higher levels of perceived privacy regulatory protection will be associated with lower levels of privacy risk concerns.
H5	Higher levels of privacy risk concerns will be associated with higher levels of protection behavior.
H6	Higher levels of privacy risk concerns will be associated with stronger preferences for regulatory protections.
H7	Larger perceived rewards will be associated with lower levels of protection behavior.
H8	Larger perceived rewards will be associated with weaker preferences for regulatory protections.
H9	The relationship between privacy risk concerns and protection behavior will be moderated by the level of perceived rewards such that larger perceived rewards will weaken the relationship.
H10	The relationship between privacy risk concerns and regulatory preferences will be moderated by the level of perceived rewards such that larger perceived rewards will weaken the relationship.

provides protection in the form of regulation. In fact, it is this premise that undergirds what has been called the "voluntary control" model of regulation [8,69], which assumes that organizations' voluntary embrace of privacy-related policies and practices will be associated with individuals' trust. In such a model, governmental regulation stands only as a backstop against the failure of such voluntary efforts. It has been noted that the privacy regulatory framework in the U.S. greatly relies on this approach [8,69].

However, although such a model is in use, we argue that individuals do not emotionally embrace it when they engage in privacy-related decision making. Although the constructs of trust and perceived regulatory protection can be logically separated (see above), we argue that—in practice—individuals emotionally connect the two. Acknowledging that this relationship is based more on our own argumentation than on previous research, we postulate the following hypothesis:

H2. Higher levels of perceived privacy regulatory protection will be associated with higher levels of trust in entities associated with information privacy.

3.3. Privacy risk concerns

Concerns associated with privacy and its risks have long assumed a central role in the majority of privacy-related studies to the point that Smith et al. [71] termed their privacy research macro-model "APCO," with "PC" standing for "Privacy Concerns." In this study, we term this central research construct "privacy risk concerns" because individuals' concerns about risks are likely the most salient attribute in a regulatory context.

We rely on the models studied by Bélanger et al. [7] and Culnan and Armstrong [20], in which trust serves as an antecedent to constructs associated with privacy concerns. Once an individual establishes trust in salient entities (which can occur via many different routes, with regulatory protection being our construct of interest in the immediate study), (s)he is likely to exhibit reduced levels of privacy risk concern because (s)he views the likelihood of negative outcomes to be reduced:

H3. Higher levels of trust in entities associated with information privacy will be associated with lower levels of privacy risk concerns.

3.4. Perceived privacy regulatory protection and privacy risk concerns

Lwin et al. [45] used power-relationship theory from sociology and social psychology to develop a model that explains individuals' perceptions of and responses to regulation. In particular, they showed that there is a strong and direct association between individuals' perceptions of legal/regulatory policies and those individuals' risk concerns regarding online activities (called "online privacy concern" in their model). Through a controlled experiment, they demonstrated that the weaker an individual perceives the privacy protection regulations in his/her own country and at an international level, the more strongly the individual perceives the risks of information being used and shared inappropriately and web activities being tracked, and the individual will respond behaviorally to those perceptions. Lwin et al. [45, p. 575] explained this as a desire to "reduce the perceived lack of equilibrium" that is associated with a perception of imbalance between perceived regulatory power and personal responsibility.

Consistent with this argument and the discussed findings, we propose the following hypothesis:

H4. Higher levels of perceived privacy regulatory protection will be associated with lower levels of privacy risk concerns.

3.5. Privacy risk concerns and protection behavior

In comparison to other information privacy topics, researchers have devoted a large amount of attention to the relationship between privacy risk concerns (sometimes using a different label for the construct) and protection behavior [71,84]. The forms of these behavioral responses can vary. For example, individuals may either embrace or resist the adoption of new technologies that protect or challenge privacy [52], submit false data [25,45,86], refuse to purchase/register at a website [25,45,50,86], request that data be removed [24,50], and/or seek additional information (e.g., privacy statement) [50,86].

With only a few exceptions, which may be attributable to saturated models with other explanatory variables (e.g., [60]) or the existence of a "privacy paradox" [55], researchers have typically found a direct link between individuals' privacy risk concerns and behavioral responses to those perceptions, even though the precise form of the behavioral responses may vary across individuals and contexts [71]. Thus, while acknowledging that some contradictions to the main body of findings exist, we propose the following hypothesis:

H5. Higher levels of privacy risk concerns will be associated with higher levels of protection behavior.

3.6. Privacy risk concerns and regulatory preferences

Compared to the prior research stream associated with H5 (above), relatively few studies have considered the relationship between privacy risk concerns and regulatory preferences, which can be defined as an individual's preferences regarding the degree

of regulatory control to enforce user control of privacy in his or her country. We note only two studies that offered substantive guidance regarding this relationship. Okazaki et al. [58] found that individuals with more concerns about risks in using mobile advertising applications prefer the government to enforce stricter regulatory controls. Earlier, Milberg et al. [49] found that a similar construct (with a different name) had the same effect on regulatory preferences. In their study, individuals who were more concerned with privacy risks indicated a stronger preference for regulation based on law than on corporate self-governance.

We expect that a similar relationship will be found in our examination of relationships with regulatory preferences:

H6. Higher levels of privacy risk concerns will be associated with stronger preferences for regulatory protections.

3.7. Perceptions of rewards

Studies based on the theory of privacy calculus (e.g., [20]) have shown that individuals may, in certain circumstances, engage in a cost-benefit analysis when making privacy-related decisions. Those studies have typically viewed costs (including risks) and rewards (in most cases, synonymous with "benefits") as being directly juxtaposed against one another in a rational calculation.

To the extent that individuals engage in a cognitive assessment of the tradeoff between costs and benefits in making privacy-related behavioral decisions, it stands to reason that individuals will be willing to give up some amount of privacy (or take more privacy-related risks) if they believe that they stand to gain from that decision. This calculus may manifest itself in protection behavior and/or in different preferences for regulatory protection. Hence, we propose the following hypotheses:

H7. Larger perceived rewards will be associated with lower levels of protection behavior.

H8. Larger perceived rewards will be associated with weaker preferences for regulatory protections.

3.8. Moderator: perceived rewards

Although traditional studies utilizing privacy calculus have considered only direct assessments of rewards and costs, a recent study [60] demonstrated a more complex relationship in which "rewards" act as a moderator in some other relationships. The earlier, simplistic juxtaposition of costs and benefits is enriched by this recent extension to the model. Therefore, we include this enhanced approach in this study.

Park et al. [60, p. 1026] found that "interactive effects are subtle and depend on levels of concern and, particularly, reward-seeking." Although their study focused on a number of linkages other than those associated with regulation, it is clear that several of their findings—in particular, that relationships between variables such as knowledge and concerns about information risks are moderated by rewards—are salient for our model. We extrapolate their findings to postulate that relationships between privacy risk concerns and outcomes (protection behavior and regulatory preferences) are more complex than are commonly realized. These relationships, while based on direct linkages, are moderated by perceptions of rewards. We postulate as follows:

H9. The relationship between privacy risk concerns and protection behavior will be moderated by the level of perceived rewards such that larger perceived rewards will weaken the relationship.

H10. The relationship between privacy risk concerns and regulatory preferences will be moderated by the level of perceived rewards such that larger perceived rewards will weaken the relationship.

4. Methods

4.1. Sampling

This study focuses on young UK people aged 18 to 25 years. This subsection of the population is known to be less wary regarding personal information than other demographic subsections [87]. As people between 18 and 25 years old have distinctive online habits and make up 11 to 16% of the European population, this group is an important object of study. Moreover, some of these young people will become key information technology (IT) decision-makers, and this generation as a whole will confront privacy-related issues to a degree that their parents' generation will not. Therefore, it is vital to study young people to gain knowledge of how these issues are perceived and the behavioral consequences. In fact, a study focusing on today's 18- to 25-year-olds provides our best opportunity to examine what will likely be widespread attitudes and behavior in tomorrow's society, particularly regarding privacy-related issues.

To date, most articles on privacy-related disclosure decisions have used U.S. samples [6], and the mix of student and consumer/professional samples has varied by topic area [6]. Pavlou [61] noted a call for "a broader diversity of sampling populations by tapping nonstudent populations outside the United States." To that end, this study uses a non-U.S. sample of both students and nonstudents.

Our data collection was done in cooperation with the European Community (EC), which funded our efforts. The terms of the data collection—including specifics of the sampling and the contents of the administered survey—were negotiated with the EC. We gratefully acknowledge the EC for their support.

4.2. Administration of the questionnaire

Data were gathered through an online survey. Invitations to participate in the survey were emailed to 140,476 UK young people,[2] who were selected through a database of European Internet users managed through the fidelity program of a French interactive marketing company, 1000mercis. We selected our sample through quotas based on data obtained from Eurostat. This enabled us to achieve a balance of genders and ages across the spectrum. We utilized this method rather than using a convenience sample because it provides greater potential for generalization, thus increasing the results' external validity. Our final sample in this study consisted of 925 UK respondents aged 18 to 25 years old who fully completed questionnaires.[3]

4.3. Description of the final sample

Table 3 shows the characteristics of the final sample. To test for nonresponse bias, a wave analysis was conducted to compare the first and last quartile of respondents in terms of demographic characteristics and key study variables [3]. The results (reported in Appendix 1) indicated that the later respondents (last quartile) were quite similar to the early respondents (first quartile) with respect to age, gender and nearly all of the constructs used in this

[2] The invitations were sent to individuals who were 15–25 years old. In this study, we omitted respondents who were 15–17 years old.

[3] Only the participants who answered the entire survey were retained here to eliminate the potential issue of missing data.

Table 3
Demographic characteristics of the sample.

Variables	Sample composition	
Age	Mean = 20.9; std. dev = 2.22; range 18–25 18–21 = 59.5%; 22–25 = 40.5%	
Gender	Female	36.6%
	Male	63.4%
Highest education level attained	Secondary school or less	47.2%
	Graduate degree	26.6%
	Postgraduate degree	10.5%
	PhD degree	1.7%
Professional activity	Student	25.8%
	Self-employed	8.5%
	Manager	13.5%
	Other white collar	10.2%
	Blue collar	4.3%
	Homemaker	4.0%
	Unemployed	6.2%
	Military/civil	3.4%
	Other	24.1%

study. Using two-tailed tests, we found that there were no differences between early and late respondents for 10 of the 13 tested constructs. We found marginally significant differences for two constructs and a significant difference for one construct. However, the *directionality* of those differences was inconsistent with what would have been observed if there had been a nonresponse bias (that is, had early/late responders perceived more/less regulatory protection and, consequently, had been less/more concerned about privacy and had engaged in less/more cautionary behavior). Thus, we conclude that nonresponse bias is not a concern in this study.

4.4. Measurement

We employed multi-item scales to measure the constructs within our theoretical model. We derived these instruments from the literature by integrating constructs from existing scales (e.g., protection behavior) or incorporating items from a previous exploratory qualitative study (e.g., regulatory preferences). Because the data collection was funded by the EC, negotiation regarding the contents of the survey instrument was necessary. In particular, the EC asked us to limit the use of multiple items to shorten the survey and use specific Likert scales for many items.[4] As a result, we were not always able to include all the survey items that we desired.

To verify their content validity, all scales were first pre-tested and validated. A two-day workshop, hosted by the EC and attended by both EC policymakers and members of the academic community, was utilized. During this workshop, all the items in the survey were discussed, and a number were revised. We then pre-tested the survey with 117 young UK subjects. This pre-testing allowed us to reformulate some questions and remove others. (See Appendix 3 for the items used in this study.)

The item measuring regulatory knowledge (RK) examined the level of a respondent's awareness regarding privacy regulation in his/her country using a 1-item, 4-point nominal scale from "I never heard about it" (1) to "I know it very well" (4).

The scale measuring perceived privacy regulatory protection (PRP) used six items that were taken from a previous EC survey on citizens' trust in ID systems and authorities [4].

The items measuring trust were developed while taking into account the digital environment, the specific focus of this study along and the previous literature on trust. We considered two different targets of trust, both the commercial entities that any user can interact with as regards personal data handling (i.e., "companies") and the entities that may offer some regulatory protection in this respect (i.e., "regulators"). Previous literature distinguished trust in public versus private entities (e.g., [51]) but mostly focused on one of these two targets (e.g., [22] considered only regulatory trust). We referenced three types of companies (a company that is well known to consumers, a company with which the user is familiar due to a previous relationship, and a company that is unknown to the user) and three regulatory institutions that can offer some support (the local council, the national government, and the European Union) to form the two main targets of trust in our model, named, respectively, "trust in companies" (TC) and "trust in regulators" (TR).

Both public opinion surveys and previous privacy literature have shown that people are significantly concerned with a range of possible privacy consequences of the spreading of their personal data. The perceived privacy risk concerns (PR) scale used in this study contains items (in a Likert format) that are used to identify the importance of two types of privacy risks that were identified in previous literature and confirmed through a preliminary exploratory study. One type addresses personal data handling that is mainly related to "data tracking" (DT), and the second addresses identity and financial fraud, which will be referred to as "identity damage" (ID). Items adapted that were from previous literature and the preliminary study form the privacy risk concerns scale used in the study, with five items for the data tracking dimension and six items for the identity damage concerns dimension.

Protection behavior (PB) is a second-order construct that distinguishes different forms of personal data protection strategies. Previous literature has been rather inconclusive regarding the different dimensions that should be differentiated in this respect. Some authors have differentiated social and technical protection (e.g., [60]), while others have considered active versus passive protection (e.g., [24]). In most cases, studies have included both technical protection and other forms of protection. We embraced this dichotomy in developing our scale. Similar to Buchanan et al. [9], we considered "technical protection" (TP) and "general caution" (GC) as two important dimensions of protection, and we added a "withholding" (WI) dimension (called "refrain" by Youn [86]). From those previous scales, we adapted a set of twelve (seven TP, three GC, and two WI) measures that people can take to protect their privacy. The items asked whether participants never (1) to always (4) used these protection measures.

Regulatory preferences (RP) refer to the preferences that a user has regarding the degree of regulatory control in his/her country (i.e., regarding governments' actions that could be implemented to enforce user control of privacy). During the workshop, we clarified the different actions that a government can take in this respect, including awareness raising (using educational or informational methods) and direct intervention (more resources, more user control, pressure on service provider). We created five items that measure the perceived efficiency of each measure on a Likert scale from 1 (not at all efficient) to 4 (very efficient).

In line with the consumer behavior literature that distinguishes between utilitarian and hedonic products [33,35] and the IS literature that distinguishes between utilitarian and hedonic information systems [80], we distinguished two types of rewards that the user can expect in exchange for his/her personal data—utilitarian and hedonic. During the expert workshop, we clarified the different benefits that a user may obtain in exchange for his/her personal data, including those that aim to provide instrumental value to the user (utilitarian rewards such as receiving money or

[4] Likert scales on the survey varied from 4 to 7 points. Previous research (e.g., [10,11,21,37,64]) has suggested that results are typically invariant across the Likert ranges used in this study.

Table 4
Construct measurement.

Construct	Scale format	Number of items	Source
Regulatory knowledge	4-point nominal scale from 'I never heard about my rights in terms of data protection' (1) to 'I know my rights ... very well' (4)	1	Developed via a preliminary exploratory study and pre-tested through an expert workshop
Perceived privacy regulatory protection	7-point Likert scale from "strongly disagree" (1) to "strongly agree" (7).	6	Taken from [4]
Trust	5-point Likert scale from "no trust at all" (1) to "very much trust" (5). Two different trust targets: companies and regulators.	6 (3+3)	Developed in relation to previous literature
Privacy risk concerns	5-point Likert scale from "not concerned" (1) to "very concerned" (5). Two dimensions of concerns: data tracking and identity damage.	11 (6+5)	Developed via a preliminary exploratory study and pre-tested through an expert workshop
Protection behavior	Second-order construct with 3 first-order dimensions depending on the type of protection used: Technical protection (e.g., using firewalls), General caution (e.g., reading privacy notices) and Withholding (e.g., not giving personal details), Self-evaluation of current and future use from "never" (1) to "always" (4).	12 (7+3+2)	Adapted from previous scales (e.g., [50])
Regulatory preferences	Perceived efficiency of different actions that could be set up by a government to enforce user control of privacy. From "not at all efficient" (1) to "very efficient" (4).	5	Developed via a preliminary exploratory study and pre-tested through an expert workshop
Perceived rewards	Likelihood to provide personal data in exchange for utilitarian versus hedonic rewards from "very unlikely" (1) to "very likely" (5).	9 (5+4)	Developed via a preliminary exploratory study and pre-tested through an expert workshop

coupons) versus those that aim to provide self-fulfilling value to the user (hedonic rewards such as connecting with friends). Five utilitarian (UR) and four hedonic rewards (HR) items were used in the final survey. Participants were asked how likely (from "very unlikely" (1) to "very likely" (5)) they were to provide personal data for each benefit (Table 4).

4.5. Data analysis method

We used a structural equation modeling (SEM) approach to validate the measures and test the proposed relationships. This method allows simultaneous examination of the measurement and structural models and provides a complete analysis of inter-relationships in the model [28]. A component-based[5] partial least squares (PLS) method was utilized to accommodate the exploratory nature of the research model, the presence of a large number of variables [38,42], and the complexity of the model. PLS is not constrained by identification concerns even if the model becomes complex, a situation that would typically restrict CB-SEM usage [31]. PLS is also preferred over CB-SEM because we focused on predicting the users' protection behavior and regulatory preferences. Furthermore, PLS path modeling is more suitable than CB-SEM for testing models with hierarchical constructs and mediating variables [14].

PLS does not automatically generate an overall goodness-of-fit index (as CB-SEM does); thus, model validity is assessed primarily by examining the structural paths and R^2 values [16]. PLS path modeling allows for the conceptualization of a hierarchical model through the repeated use of manifest variables (i.e., the higher order component uses all indicators of the lower order components [30,43,54,77,83]). Lohmöller [43] showed that this indicator reuse approach is suitable for the analysis of hierarchical component models in PLS. We constructed the reflective, hierarchical construct model in PLS path modeling using the two steps below:

(1) We constructed the first-order latent variables (trust—in companies and in regulators; privacy risk concerns—data tracking and identity damage; perceived rewards—utilitarian and hedonic; protection behavior—technical, general caution and withholding) and related them to their respective block of manifest variables using reflective indicators in the measurement model.
(2) We then constructed the second-order latent variables (trust, privacy risk concerns, perceived rewards, and protection behavior) by relating them to the blocks of the underlying first-order latent variables, which are viewed as reflective indicators for these second-order latent variables.[6]

5. Results

Structural equation models should be analyzed in two stages: the measurement model and the structural model [2]. The estimates of the measurement model, which consists of the relationships between constructs and the indicators used to measure them, allow us to assess the psychometric properties of the scales.

We used SmartPLS 3.1 [65] to estimate the parameters in the measurement and structural models using a path weighting scheme for the inside approximation [12,13,77]. We also used the standard bootstrapping procedure implemented in SmartPLS with 500 replications to obtain the standard errors of the estimates.[7]

5.1. Test for common method bias

We first checked for common method bias (CMB) in our data. CMB can be addressed a posteriori through statistical analysis [62]. We used two methods to statistically assess CMB.[8]The first

[5] Other SEM techniques (in particular, those using AMOS or LISREL software packages) are covariance-based (called "CB-SEM").

[6] The loadings of the first-order factors on the second-order factors were as follows: for trust: trust in companies (0.812) and trust in regulators (0.925); for privacy risk concerns: data tracking (0.953) and identity damage (0.931); for perceived rewards: utilitarian (0.946) and hedonic (0.937); for protection behavior: technical protection (0.962), caution (0.745) and withholding (0.505).

[7] We used "Bias-Corrected and Accelerated (BCa) Bootstrap" because it is the most stable method that does not need excessive computing time.

[8] Liang et al.'s [42] technique is largely used in IS research. See Chin et al. [15] for an assessment of the approach.

approach—which is increasingly disputed ([63], Appendix) but still widely reported (e.g., [36,53,59,81])—employed Harman's single-factor test [62]. All the variables submitted to an exploratory factor analysis (EFA), and the unrotated factor solution was examined. Common method bias may exist if (1) a single factor emerges from the unrotated factor solution or (2) one general factor accounts for the majority of the covariance in the variables [62]. Neither of these outcomes occurred here, suggesting that CMB should not be an issue in this study. We also followed the approach used, for example, by Liang et al. [42]. Using SmartPLS, we specified a method factor together with the original latent variables in the measurement model, and we calculated the squared factor loadings for both the method factor and the substantive factors (i.e., original latent variables). The average variance explained by the substantive factors was approximately 0.70 while that explained by the method factor was approximately 0.06, thus confirming that common method bias is not a concern in our study (see Appendix 2).

5.2. Measurement model: instrument validation

Measurement model assessment involves examining individual indicator reliabilities (through the squared standardized outer loadings), the reliabilities for each construct's composite of measures (i.e., internal consistency reliability using the composite reliability scores), and the measures' convergent (using the average variance extracted, AVE) and discriminant (using the Fornell–Larcker criterion and the cross-loadings) validities.

After removing some items with very low factor loadings or high cross-loadings, the reliability, convergent validity, and discriminant validity of the instrument were first examined. Appendix 4 shows that all but one of the remaining loadings are larger than the suggested threshold of 0.70 [12]. One item for regulatory preferences (RP3) has a loading of 0.61. In general, standardized loadings of 0.70 or greater are needed for the shared variance between each item and its construct to exceed the error variance, but loadings of 0.60–0.70 are often considered acceptable if the loadings of other items within the same construct are high [12,13]. Thus, we retained all the items.

Table 5 shows that all composite reliabilities are larger than the suggested 0.70, and all AVE values are greater than the suggested 0.50, indicating that the measurement model has good convergent validity [28]. For sufficient discriminant validity to be present, items should load more strongly onto their own constructs, and the average variance shared between each construct and its measures should be greater than the variance shared between the construct and other constructs [17]. Appendix 5 shows that items load much more highly onto their own latent constructs than onto any other latent constructs (cross-loadings). In addition, the AVE square roots are larger than the correlations among constructs (Table 6). Therefore, discriminant validity is achieved.

5.3. Structural model: hypotheses tests

As the measurement model evaluation provided evidence of reliability and validity, we now turn to an examination of the structural model estimates. The primary criterion for this structural assessment is the coefficient of determination (R^2), which represents the amount of explained variance by each endogenous latent variable. Standardized path coefficients provide other evidence of the structural model's quality, and their significance is assessed using resampling procedures.

A structural model with the effects hypothesized in our conceptual model was examined. The results of this model and of hypotheses testing are summarized in Table 7 and Fig. 2. Eight of the ten hypotheses are validated, and the model explains 10% of the variance in privacy risk concerns, 21.3% in trust, 12.9% in protection behavior, and 8.6% in regulatory preferences. Regarding these percentages, recall that we do not claim that our model is exhaustive given the paucity of theoretical development in this research domain. As will be discussed in Section 6.2.2, future studies can estimate more complex models with additional constructs.

We assumed that perceived privacy regulatory protection would be negatively influenced by awareness of privacy regulation; this assumption is upheld ($b = 0.075$, $t = 2.132$), supporting H1. We also predicted that trust (both in regulators and in companies) would be positively influenced by perceived privacy regulatory protection and found that this is indeed the case ($b = 0.460$, $t = 14.973$), supporting H2. Trust itself expected to negatively influence privacy risk concerns, and we validate this effect ($b = -0.100$, $t = 2.839$), confirming H3. Perceived privacy regulatory protection was predicted to also directly and negatively influence privacy risk concerns; this influence is found ($b = -0.253$, $t = 6.418$), supporting H4. Privacy risk concerns were, in turn, predicted to influence both dependent variables. We found that privacy risk concerns indeed influences both protection behavior ($b = 0.227$, $t = 6.063$) and regulatory preferences ($b = 0.229$, $t = 6.379$), supporting H5 and H6. The

Table 5
Statistics for constructs.

	Number of items	Mean	Std. Dev.	CR	AVE	R^2	Cronbach's alpha
RK	1	2.75	0.842	–	–	–	–
PRP	6	3.18	1.37	0.935	0.707	0.005	0.917
TR	3	3.42	1.16	0.951	0.866	0.857	0.919
TC	2	2.67	0.90	0.951	0.906	0.661	0.893
DT	6	3.20	0.79	0.939	0.719	0.908	0.921
ID	5	1.74	0.85	0.933	0.736	0.867	0.910
UR	5	3.22	0.92	0.892	0.624	0.894	0.849
HR	4	3.40	0.91	0.911	0.721	0.877	0.869
TP	7	2.93	0.78	0.914	0.604	0.925	0.890
GC	2	2.33	0.90	0.882	0.788	0.555	0.733
WI	2	2.57	0.66	0.803	0.670	0.255	0.509
RP	5	3.05	0.58	0.869	0.572	0.086	0.810

RK, regulatory knowledge; PRP, perceived privacy regulatory protection; TR, trust in regulators (trust—Dimension 1); TC, trust in companies (trust—Dimension 2); DT, data tracking (privacy risk concerns—Dimension 1); ID, identity damage (privacy risk concerns—Dimension 2); UR, utilitarian rewards (rewards—Dimension 1); HR, hedonic rewards (rewards—Dimension 2); TP, technical protection (protection behavior—Dimension 1); GC, general caution (protection behavior—Dimension 2); WI, withholding (protection behavior—Dimension 3); RP, regulatory preferences.

Table 6
Correlations and squared roots of AVEs.

	RK	PRP	TR	TC	DT	ID	UR	HR	PB	GC	WI	RP
RK	**1.000**											
PRP	0.072	**0.841**										
TR	−0.038	0.449	**0.931**									
TC	−0.044	0.341	0.530	**0.952**								
DT	0.130	−0.311	−0.235	−0.167	**0.848**							
ID	0.087	−0.256	−0.172	−0.111	0.776	**0.858**						
UR	−0.056	0.298	0.365	0.395	−0.141	−0.022	**0.790**					
HR	0.009	0.262	0.328	0.366	−0.039	0.013	0.772	**0.849**				
PB	0.321	−0.081	−0.207	−0.134	0.249	0.202	−0.241	−0.197	**0.777**			
GC	0.216	0.033	−0.107	−0.127	0.120	0.132	−0.167	−0.155	0.584	**0.888**		
WI	0.144	−0.115	−0.210	−0.145	0.195	0.129	−0.269	−0.262	0.349	0.292	**0.819**	
RP	0.048	−0.025	0.054	0.105	0.231	0.188	−0.122	−0.182	0.139	0.084	0.049	**0.756**

Bolded values indicate the squared roots of the AVEs.

model also predicted a direct effect of perceived rewards on both protection behavior and regulatory preferences. We found that perceived rewards (both utilitarian and hedonic) have a significant negative influence on protection behavior ($b = -0.240$, $t = 6.923$); in other words, the more the person is expecting rewards in exchange for his/her data, the less (s)he tends to embrace any specific self-protection behavior, validating H7. This result supports the privacy calculus process—that is, if the individual perceives that there is some benefit to disclose data (especially if the benefits exceed the risks to do so), (s)he will be less interested in self-protecting his/her data. We also found that perceived rewards have a significant negative influence on regulatory preferences ($b = -0.173$, $t = 4.693$), validating H8. The more the individual is expecting rewards in exchange for his/her data, the less (s)he is looking for help from the government to give him/her control of his/her data. Finally, we predicted an interaction effect between rewards and privacy risk concerns on protection behavior and regulatory preferences, respectively, H9 and H10. Although perceived rewards and privacy risk concerns both directly influence protection behavior and regulatory preferences, the interaction effects are not significant.

5.4. Mediation tests

Mediation in path models can be assessed by examining the relationship of the direct link (denoted as c) between two variables and the indirect link via the potential mediator variable (denoted as path a from the predictor to the mediator and as path b from the mediator to the endogenous variable). Mediation can be assumed if the indirect effect $a \times b$ is significant (i.e., if H_0: $a \times b = 0$ can be rejected). The asymptotical normally distributed z-statistic can be used as a test: if the z-value exceeds 1.96 (at $p < 0.05$), then the null hypothesis can be rejected (i.e., there is no indirect effect) [74]. We calculated the z-statistic for each of the mediating effects present in our model. The results appear in Table 8.

We found that perceived regulatory protection significantly mediates the effect between regulatory knowledge and both trust ($z = 2.007 > 1.96$) and privacy risk concerns ($z = |-1.970| > 1.96$), consistent with the reported results (in Table 7) for H1 and H3. In addition, we confirmed that trust is a significant mediator between perceived regulatory protection and privacy risk concerns ($z = |-2.422| > 1.96$), consistent with our reported findings (in Table 7) for H2, H3 and H4. Finally, we confirmed that privacy risk concerns are a significant mediator between perceived regulatory protection and both protection behavior ($z = |-4.845| > 1.96$) and regulatory preferences ($z = |-4.527| > 1.96$), consistent with our results for H4 to H6.

5.5. Post hoc analysis on the influence of previous experience

Privacy perceptions in general and especially regulatory perceptions are often inferred from individual knowledge or previous experience [71]. Our results clearly show the impact of knowledge on perceived regulatory protection, validating H1. To assess whether previous experience influences other parts of our model, we divided our sample into two groups related to their Internet experience on the basis of developed skills (see items in Appendix 3)—that is, the activities that each respondent reported engaging in online from a list of eight classic activities (e.g., instant messaging, sharing pictures or videos, keeping a blog, checking

Table 7
Tests of hypotheses.

Hyp.	Paths	Beta	St. Dev.	*t* Statistics	*p*-value	Result
H1	Regulatory knowledge → Perceived regulatory protection	0.075	0.034	2.132	*	Supported
H2	Perceived regulatory protection → Trust	0.460	0.031	14.973	***	Supported
H3	Trust → Privacy risk concerns	−0.100	0.035	2.839	**	Supported
H4	Perceived regulatory protection → Privacy risk concerns	−0.253	0.040	6.418	***	Supported
H5	Privacy risk concerns → Protection behavior	0.227	0.037	6.063	***	Supported
H6	Privacy risk concerns → Regulatory preferences	0.229	0.035	6.379	***	Supported
H7	Rewards → Protection behavior	−0.240	0.035	6.923	***	Supported
H8	Rewards → Regulatory preferences	−0.173	0.039	4.693	***	Supported
H9	Privacy risk concerns * Rewards → Protection behavior	−0.108	0.053	1.558	>0.05	Not Supported
H10	Privacy risk concerns * Rewards → Regulatory preferences	−0.034	0.120	0.772	>0.05	Not supported

* $p < 0.05$.
** $p < 0.01$.
*** $p < 0.001$.

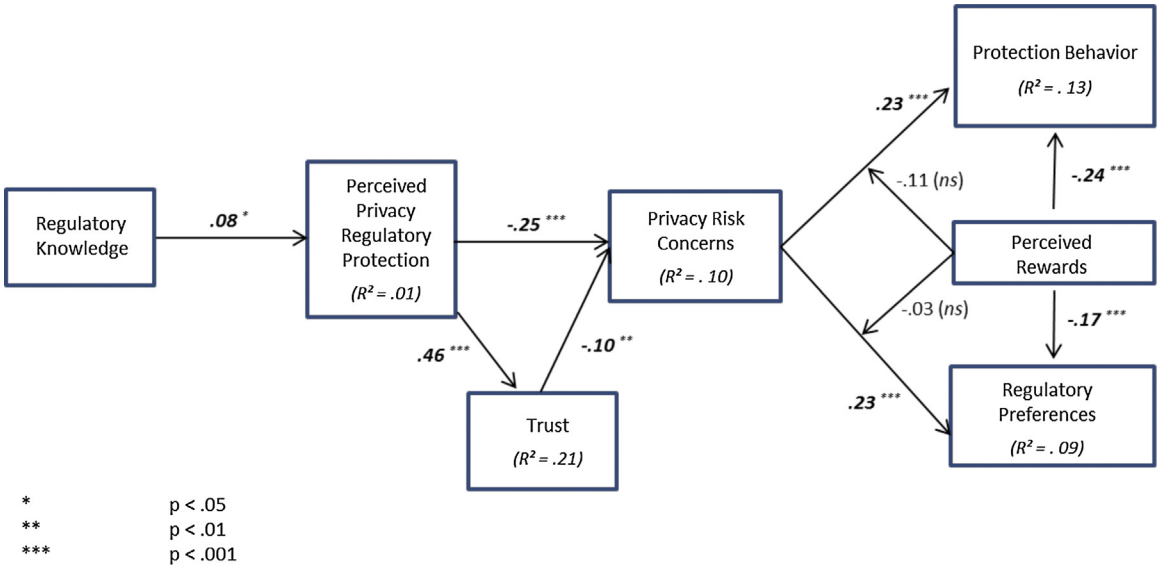

Fig. 2. Results model.

emails). The two groups are called, respectively, "Basic" (people engaging in only classic online activities such as checking emails and using a search engine) and "Advanced" (people engaging extensive functions on the Internet and social networking sites). We then conducted a multi-group analysis using SmartPLS 3.0 by comparing our model and the corresponding path coefficients between Basic (Bas) and Advanced (Adv) individuals. The results are shown in Table 9.

Two paths are clearly impacted by the respondents' Internet experience. First, the influence of perceived regulatory protection on trust is higher for individuals who use the Internet for advanced tasks ($b = 0.552$ for Advanced vs. $b = 0.435$ for Basic, $p = 0.042$). Second, there is a significant difference between Basic and Advanced individuals regarding the influence of perceived rewards on regulatory preferences ($p = 0.033$): the influence of perceived rewards is massive for Advanced individuals but nonsignificant for Basic individuals. We therefore found some support for the role of experience in influencing privacy perceptions and behavior, especially regarding regulation, confirming some assertions from previous literature [58]. The influence is not general, however; rather, it is specific to the links between perceived regulatory protection and trust and between rewards and regulatory preferences.

6. Discussion

This study makes three important contributions to the privacy literature.

First, the study is the first to construct a consolidated model that addresses a number of constructs related to governmental regulations and outcomes that have only been considered separately in previous research [25,40,45,49,58,79,82,85]. These studies have, independently, identified some variables and relationships that may explain a number of perceptions, attitudes, and behaviors associated with privacy regulation. In this paper, we have looked across these articles to identify common components in their analyses.

Second, this paper provides empirical justification for relationships between several constructs that had heretofore been untested. We have tested a model that considers relationships between an antecedent variable (regulatory knowledge); a mediating structure that encompasses perceived privacy regulation protection, trust,

Table 8
Tests for mediation.

	Mediation effect 1	Mediation effect 2	Mediation effect 3	Mediation effect 4	Mediation effect 5
Mediator tested	Perceived regulatory protection	Perceived regulatory protection	Trust	Privacy risk concerns	Privacy risk concerns
DV	Trust	Privacy risk concerns	Privacy risk concerns	Protection behavior	Regulatory preference
Path (a)	Regulatory knowledge → Perceived regulatory protection	Regulatory knowledge → Perceived regulatory protection	Perceived regulatory protection → Trust	Perceived regulatory protection → Privacy risk concerns	Perceived regulatory protection → Privacy risk concerns
Path (b)	Perceived regulatory protection → Trust	Perceived regulatory protection → Privacy risk concerns	Trust → Privacy risk concerns	Privacy risk concerns → Protection behavior	Privacy risk concerns → Regulatory preferences
(a)	0.071	0.071	0.467	−0.274	−0.274
(b)	0.467	−0.274	−0.086	0.249	0.224
Direct effect (c)	−0.079	0.133	−0.274	0.089	−0.006
Indirect effect ($a \times b$)	0.033	−0.019	−0.040	−0.068	−0.061
Total effect ($a \times b + c$)	−0.046	0.113	−0.314	0.021	−0.067
z	$2.007 > 1.96$	$\|-1.970\| > 1.96$	$\|-2.422\| > 1.96$	$\|-4.845\| > 1.96$	$\|-4.527\| > 1.96$

Table 9
Multi-group test for the impact of Internet experience.

Paths	Path coeff. (Adv)	Path coeff. (Bas)	CI low (Adv)	CI low (Bas)	CI high (Adv)	CI high (Bas)	Path coefficients-diff |Adv–Bas|	*p*-Value (Adv vs. Bas)	Sig.
Regulatory knowledge → Perceived regulatory protection	0.120	0.023	0.019	−0.095	0.219	0.132	0.097	0.116	n.s.
Perceived regulatory protection → Trust	0.552	0.435	0.481	0.316	0.645	0.531	0.117	**0.042**	<5%
Trust → Privacy risk concerns	−0.184	−0.071	−0.332	−0.187	−0.082	0.043	0.113	0.908	n.s.
Perceived regulatory protection → Privacy risk concerns	−0.228	−0.323	−0.350	−0.449	−0.102	−0.230	0.096	0.128	n.s.
Privacy risk concerns → Protection behavior	0.284	0.173	0.172	0.051	0.367	0.285	0.112	0.083	n.s.
Privacy risk concerns → Regulatory preferences	0.158	0.152	0.036	0.060	0.262	0.274	0.006	0.475	n.s.
Perceived rewards → Protection behavior	−0.238	−0.252	−0.310	−0.335	−0.074	−0.082	0.014	0.434	n.s.
Perceived rewards → Regulatory preferences	−0.248	−0.072	−0.043	0.146	−0.313	−0.110	0.176	**0.033**	<5%
Privacy risk concerns × Perceived rewards → Protection behavior	−0.176	−0.129	−0.446	−0.481	−0.219	−0.216	0.047	NA	n.s.
Privacy risk concerns × Perceived rewards → Regulatory preferences	0.159	−0.307	0.238	−0.547	0.438	0.490	−0.148	NA	n.s.

Bolded *p*-values are significant at $p < 0.05$.

and privacy risk concerns; two outcome variables (protection behavior and regulatory preferences); and direct and moderating effects of perceived rewards. Although our model does not provide an exhaustive test of all antecedents, mediators, and outcome variables [71], it is the first to look across that spectrum of relationships by considering some selected variables within each domain associated with privacy regulation.

Third, this study provides a starting set of measurement scales that can be used by future researchers as they delve more deeply into four constructs that had been given only limited attention in prior research—regulatory knowledge, privacy risk concerns, regulatory preferences, and perceived rewards—and their relationships. While we do not claim that our newly developed measures have been subjected to an exhaustive process of construct identification and measurement [75,76], our initial efforts to bound and measure these constructs should enlighten researchers who conduct additional studies in this domain.

Our findings were generally consistent with our predictions, with only two of our hypotheses (H9 and H10) failing to find support. Those two hypotheses predicted moderating effects of perceived rewards on two of the model's direct relationships (between privacy risk concerns and protection behavior and between privacy risk concerns and regulatory preferences, respectively). Any moderating influence of perceived rewards is obviously overshadowed by the strong direct relationships between the other constructs. It is clear, however, that perceived rewards have strong direct effects on both protection behavior and regulatory preferences, which demonstrates the importance of this construct in the overall model. We conclude that the role of perceived rewards deserves much additional attention, as we will note below in our discussion of future research initiatives.

Before turning to a discussion of the implications for research and practice, we will highlight some limitations of this study.

6.1. Limitations

While this study makes important contributions to the literature, we note three areas that can arguably be considered limitations, and we offer suggestions for ways in which future research might take advantage of targeted extensions to our approach.

First, the study's sample—while gathered through an independent data source—is based in one country (the UK) and is bounded by the 18–25 year age demographic. As noted earlier, this age group is ideal for the study of the phenomena addressed by our model. However, caution must be taken in generalizing the results to other age groups. One obvious extension to increase the study's generalizability would be to secure a sample across a broader domain, especially one that covers subjects across the age spectra.

Strictly from the standpoint of generalizability, it may not be necessary to obtain a multi-country sample, as numerous studies have drawn conclusions from single-country samples. However, to the extent that cultural values within a given society may impact either the constructs or the relationships between them, it would be fruitful to examine those cultural impacts. This would be most readily achieved by comparing samples (using the same instrument and gathered through the same sampling methodology) from several cultures. At the time the data are gathered for the constructs in this study, subjects' responses to cultural value scales (e.g., [34]) could also be elicited. Such an approach is far preferable to one in which it is simply assumed that all members of a certain culture share the same values. By hypothesizing both impacts on the constructs themselves and on their relationships a priori,

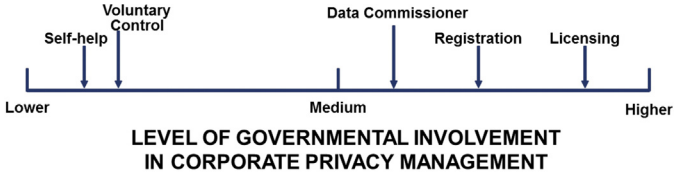

Fig. 3. Regulatory models. (1) The Self-Help model depends on data subjects' challenging record keeping practices by identifying perceived problems and bringing them to the courts for resolution. The United States relies to some degree on this model. (2) The Voluntary Control model relies on self-regulation by corporate entities. Each firm ensures its own compliance. The United States also relies to some degree on this model. (3) The Data Commissioner model creates a governmental institution that embraces the role of an ombudsperson. The commissioner receives complaints and investigates them. The commissioner offers advice and makes proposals regarding legislation; it may also inspect some information processing operations. Germany relies on this model. (4) The Registration model requires that each databank containing personal data be *registered* (typically upon payment of a fee) *by a governmental institution* (the Registrar). The Registrar cannot block the creation of a particular information system but can "deregister" a system based on a complaint and investigation. The UK relies on this model. (5) The Licensing model requires that each databank containing personal data be licensed (typically upon payment of a fee) by a governmental institution. This institution would stipulate specific conditions for the collection, storage, use, and re-use of personal data. This model requires *prior* approval for any re-use of data. Sweden relies on this model.
Sources: Categories based on [8]. Interpretations based on [8,49,69]. See [49] for country classifications.

researchers could ascertain which portions (if any) of the model are culturally impacted.

Similarly, a multi-country sample would enable the consideration of different regulatory models and how they may impact individuals' perceptions and preferences across countries. As was originally documented by Bennett [8] and later consolidated by Milberg et al. [49], countries' regulatory approaches can be largely classified into one of five models, as shown in Fig. 3.

A multi-country sample, if constructed carefully, would allow tests of the association between an additional independent variable (i.e., regulatory model in a subject's country) and subjects' perceptions of regulatory protection. It is generally assumed by regulators that the models on the right-hand side of Fig. 3 (which are generally observed in countries within the European Union, in Canada, and in some countries in Asia) provide higher levels of privacy protection than do those on the left-hand side of Fig. 3 (the U.S.-based models). These levels of protection, if perceived by individuals within those countries, should be associated with individuals' behavior in privacy-related decision making, assuming the validity of the model that was confirmed in this study. This extension to the current study—which would, of course, require a far larger sample drawn from multiple countries—would stand as a major contribution to the literature stream.

Second, because the data collection for this study was gathered in collaboration with the EC, we were unable to dictate the content of the survey, including the wording of the measurement items. All items on the survey were the result of discussion and compromise between the authors and the EC. As a result, we were sometimes constrained in our ability to employ scales that—while perhaps not isomorphic to the narrow constructs in our model—had previous validation in other studies (e.g., [72]). The impact of this limitation is modest, however, because previously validated instruments do not exist for many of the constructs in our model, even in tangentially related forms. Consequently, for those constructs for which no validated scales existed, we were forced to develop measurement items using pilot testing and modifications as appropriate. Although our efforts were consistent with those embraced in most studies of this nature, we nevertheless recommend that researchers view the items used in this study as a "starting set" for validation.

The process for full creation and validation of an instrument is complex, and it involves the bounding of the construct, numerous pilot tests, evaluation for nomological validity, etc. (see [75,76]). We hope that researchers will embrace the goal of providing rigorously validated instruments for these constructs.

Third, as with the vast majority of previous privacy-related studies, this study shows *correlation* but not *causality*. However, the model can be extended to determine which changes in certain constructs *cause* changes in others.

To facilitate such findings, laboratory controls and treatments will be required in an experimental setting. For example, an experiment might be designed to expose randomly assigned subjects to different scenarios in which their confidence in online domains is manipulated. Additionally, they might receive different treatments that would manipulate their perceptions of privacy regulation protection. Following those manipulations, their levels of trust, perceived regulatory protection, privacy risk concerns, and perceived rewards (which can be expected to vary based on their treatment) would be measured, and their actual behavior can be observed and recorded. To the extent that differences in these behavioral variables were observed across treatment cells, one can reasonably infer that the treatments caused the differences in behavior.

One subtle attribute of such controlled experiments is that because the subjects are assigned randomly to the treatment cells, the sampling mechanism within the population is less critical than it is for a survey study. Generalizability is gained through the treatment protocol rather than through the sampling.

6.2. Implications for research

In addition to conducting studies that extend sampling to other demographics and countries, that further the development of measures, and that include experiments that enable inferences about causality (see above), researchers may extend this stream of research in other ways.

6.2.1. The roles of perceived rewards and previous experience

It is apparent that the construct of perceived rewards has an important effect on some of the other constructs in this model. However, its specific relationship with these constructs (and with the relationships between them) deserves additional attention. Although some of our suppositions (direct effects on protection behavior and regulatory preferences) were supported, our other suppositions—that perceived rewards would interact with other variables to moderate some relationships—did not find support in this study. This suggests that the cost-benefit analysis that undergirds the privacy calculus model (e.g., [20]), while not well integrated into the overall privacy literature stream (see [71]), provides a fruitful path for future research.

We suggest that future studies examine the respective roles of both tangible and intangible rewards and how they may impact—both directly and indirectly—other variables in models such as that tested in this study. It is certainly conceivable that different forms of perceived rewards might have different direct and moderating influences, and these influences might even be contextual, with differing gradations for different types of data (e.g., financial, medical, purchase records) or situations. The combinations of such effects may reveal a complex domain with rich research opportunities for the future.

Through an exploratory post hoc analysis, we also found an interesting dichotomy between previous online experiences and the strength of some of the relationships in this study's model. In particular, it appears that some of the relationships in the studied model are more robust for "Advanced" than for "Basic" Internet users. This suggests that future researchers could benefit from including both direct and moderating effects of previous experiences in their data collection and modeling efforts. Note that this concept of previous experience is in addition to, and not a substitute for, the concept of prior negative experiences, which has occasionally been considered by other researchers (e.g., [58]).

6.2.2. Expanding the model with additional constructs

We also reflect once again on the origin of the basic model tested in this study: previous studies that have considered governmental regulation and outcomes at the individual unit of analysis [25,40,45,49,58,79,82,85]. Our model (see Fig. 1) does not purport to represent an exhaustive set of all the variables that had been considered previously, and some recent articles that have reviewed the broader domain of privacy research [6,41,71] reference a very large set of over two dozen antecedent constructs and approximately ten mediating or moderating variables, many of which may have an impact on behavior and regulatory preferences. It is obvious that numerous additional combinations of constructs can be considered within this same basic model. Factors such as individual personality traits, previous life

experiences, one's cultural indoctrination, and/or one's exposure to various forms of regulation (see above) may serve as antecedents to preferences for regulatory protections. Note there may be additional moderating variables (in addition to perceived rewards, which we considered in H9 and H10) that moderate those relationships.

Of course, no single study can provide an exhaustive set of all the combinations, but it remains clear that several years of research studies can be identified in such a super-set. We urge researchers to carefully consider tests of other combinations.

6.2.3. Process model

Similar to nearly all the previous studies on privacy-related topics, this study tested a *variance* model. Variance models explore relationships between higher and lower values within certain constructs using a cross-sectional design. They do not focus on the passage of time or on events that lead to changes of state.

Yet, another entire domain of research awaits interested researchers: *process* models of privacy-related behavior. A largely unexplored domain of research (indeed, only a few examples such as [70,73] exist), process modeling can provide a rich understanding of the changes that occur in privacy-related relationships over time.

Generally speaking, process modeling requires a long-term research commitment to data gathering. Often through interviews, researchers attempt to clarify the trigger events that lead to different states of perception or behavior. Typically, process modeling is done in an organizational context, although it is certainly conceivable that researchers could attempt such a study at an individual, dyadic, or small group level.

With respect to privacy-related regulatory phenomena, a fruitful process modeling initiative might involve an examination of changes in individuals' levels of trust and their perceptions of regulatory protection, risks, and rewards over time. Additionally, one can track changes in their behavior and preferences regarding regulation. If this is done along with a similar tracking process of changes in regulation at the national level (or within the EC at the commission level), rich insights might emerge. One can envision, for example, a long-term interview schedule that allowed a researcher to follow individuals as they experienced changes in privacy regulation along with modifications to commercial offerings that had privacy-related attributes. How the individuals perceived the changes, and how their behavior and regulatory preferences changed in response, would reveal deep complexities and associations.

6.3. Implications for managerial practice

This study's major contributions are to the privacy research stream; nevertheless, there are two implications for practice that should be noted.

First, this study makes clear that individuals do not draw privacy-related conclusions in isolation: their approaches to protection behavior and privacy preferences can in some measure be predicted based on other constructs. Thus, managers would be well served to consider how their organizational decisions may lead stakeholders to perceive risk and rewards. Although these perceptions are cumulative to some degree—that is, they are not necessarily specific to one particular firm or organization—there is some room for managers to influence individuals' behavioral calculations and even the extent to which they may demand regulatory protections.

Second, as noted earlier, we intentionally recruited a sample of young consumers for this study in light of their high use of digital technologies and their future role as decision-makers. It should therefore be instructive to note that these young people perceive real risks in online interactions. Furthermore, these perceptions manifest themselves in individuals' protection behavior and, to some extent, regulatory preferences. This should serve as a "call to arms" as we consider these individuals' reactions as new technologies emerge in future decades.

6.4. Implications for regulation

It is also obvious that this study's findings can have implications for privacy regulation. Although this study's sample included subjects from only one country (the UK), the strong support for the relationship between perceived privacy regulation protection and privacy risk concerns (H4), coupled with the strong support for the consequent relationship with protection behavior (H5), suggests that individuals may ultimately feel a reduced need to engage in their own protection behavior—which can thwart some commercial initiatives—if they become convinced that their countries' regulatory systems protect them.

As shown above (in Fig. 3), the UK's Registration model largely provides such protection, but an additional model (Licensing) is even more stringent in that context. It might reasonably be conjectured that commercial activities would be more efficient if regulatory protections were provided proactively at a systemic level (via governmental entities) than left to individuals' reactive responses. To the extent that commercial entities can know, in advance of offering new products or services, of any constraints on their collection, use, and re-use of personal information, this may well be preferable to responding to customers' individualistic behavioral choices. Legal ambiguity is likely reduced via the more stringent regulatory models in Fig. 3, even though certain data collection and (re-)use practices may be restricted under such models.

7. Conclusion

With data collection increasing at a rapid rate in all industrialized societies, individuals' privacy-related behavior and regulatory preferences are becoming subjects of increasing interest to marketers, policymakers, and many other societal stakeholders. It is heartening that the privacy research stream has grown over the past few years and that some attempts are now being made to consolidate disparate findings into overarching models.

In this study, we have tested a model that incorporates some of the relevant constructs associated with privacy regulation that have been posited to explain privacy-related behavior and regulatory preferences. This study should not be viewed as an exhaustive test of a macro-model. Rather, it should be viewed as one step on a long path of research initiatives that will yield additional understanding over time in this important domain. We hope that other researchers will join us in future research initiatives that unpack these complex relationships.

Funding

This study was funded by the European Commission 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 1. Tests for nonresponse bias

T-tests of mean differences for first and fourth quartile responses.

Construct (see Table 5)	Mean differences (1st and 4th quartiles—earliest and latest responses)	Standard error	*t*-value	Significance (two-tailed)
PRP	−0.23304	0.12430	−1.875	$p < 0.10$
TR	0.12425	0.10605	1.172	n.s.
TC	0.07227	0.09128	0.792	n.s.
DT	−0.22294	0.02475	−9.009	$p < 0.01$
ID	0.10216	0.06479	1.577	n.s.
UR	0.10292	0.07711	1.335	n.s.
HR	−0.08735	0.07633	−1.144	n.s.
TP	0.03711	0.07129	0.521	n.s.
GC	0.12361	0.06808	1.816	$p < 0.10$
WI	0.02814	0.05797	0.485	n.s.
RP	0.04502	0.05264	0.855	n.s.
Age	−0.267	0.211	−1.267	n.s.

Chi-square test for gender

% male 1st quartile (earliest responses)	% male 4th quartile (last responses)	Chi-square (Pearson)	Significance (two-tailed)
49.5%	50.5%	0.089	n.s.

Appendix 2. Test for common method bias (CMB)

Construct	Indicator	Item factor loadings	Variance explained by the factors	Method factor loadings	Variance explained by the methods
Regulatory knowledge	RK	1	1.000	0.154	0.024
Perceived regulatory protection	PRP1	0.772	0.596	−0.404	0.163
	PRP2	0.837	0.701	−0.227	0.052
	PRP3	0.877	0.769	−0.269	0.072
	PRP4	0.824	0.679	−0.29	0.084
	PRP5	0.871	0.759	−0.268	0.072
	PRP6	0.859	0.738	−0.257	0.066
Trust in regulators	TR1	0.908	0.824	−0.271	0.073
	TR2	0.951	0.904	−0.251	0.063
	TR3	0.932	0.869	−0.236	0.056
Trust in companies	TC1	0.952	0.906	−0.287	0.082
	TC2	0.952	0.906	−0.248	0.062
Data tracking concerns	DTC1	0.813	0.661	0.212	0.045
	DTC2	0.897	0.805	0.239	0.057
	DTC3	0.899	0.808	0.233	0.054
	DTC4	0.813	0.661	0.29	0.084
	DTC5	0.805	0.648	0.293	0.086
	DTC6	0.855	0.731	0.268	0.072
Identity damage concerns	IDC1	0.835	0.697	0.241	0.058
	IDC2	0.846	0.716	0.225	0.051
	IDC3	0.891	0.794	0.209	0.044
	IDC4	0.866	0.750	0.294	0.086
	IDC5	0.852	0.726	0.291	0.085
Utilitarian rewards	UR1	0.732	0.536	−0.268	0.072
	UR2	0.714	0.510	−0.232	0.054
	UR3	0.807	0.651	−0.256	0.066
	UR4	0.854	0.729	−0.261	0.068
	UR5	0.838	0.702	−0.221	0.049
Hedonic rewards	HR1	0.843	0.711	−0.216	0.047
	HR2	0.904	0.817	−0.229	0.052
	HR3	0.888	0.789	−0.239	0.057
	HR4	0.752	0.566	−0.367	0.135
Technical protection	TP1	0.835	0.697	0.24	0.058
	TP2	0.832	0.692	0.249	0.062
	TP3	0.704	0.496	0.298	0.089
	TP4	0.726	0.527	0.222	0.049
	TP5	0.769	0.591	0.224	0.050
	TP6	0.742	0.551	0.212	0.045
	TP7	0.82	0.672	0.259	0.067
General caution	GC1	0.888	0.789	0.284	0.081
	GC2	0.888	0.789	0.313	0.098

Appendix 2 (*Continued*)

Construct	Indicator	Item factor loadings	Variance explained by the factors	Method factor loadings	Variance explained by the methods
Withholding	W1	0.818	0.669	0.347	0.120
	W2	0.82	0.672	0.298	0.089
Regulatory preferences	RP1	0.809	0.654	0.162	0.026
	RP2	0.791	0.626	0.124	0.015
	RP3	0.61	0.372	0.018	0.000
	RP4	0.781	0.610	0.116	0.013
	RP5	0.772	0.596	0.072	0.005
Average		0.834	0.701	0.023	0.064

Appendix 3. Survey items and statistics

For each of the following statements, please state if you tend to agree or not	Scale	Mean	SD
Perceived regulatory protection (PRP)			
In UK, my personal data are properly protected	1–7	3.57	1.638
UK legislation can cope with the growing number of people leaving personal information on the Internet	1–7	3.05	1.569
I believe that the systems used by the public authorities to manage the citizens' personal data are technically secure.	1–7	3.09	1.635
I believe citizens will be able to keep a good level of control over their personal data	1–7	3.29	1.581
I will always be able to rely on public authorities for help if problems arise with my personal data	1–7	2.97	1.628
I believe that the authorities that manage my personal data are professional and competent	1–7	3.09	1.652

Overall, how much do you trust the following institutions to handle your personal information safely?	Scale	Mean	SD
Trust in regulators (TR)			
The national government	1–5	3.47	1.297
The European Union	1–5	3.47	1.271
The Local Council	1–5	3.32	1.204

Overall, how much do you trust the following entities to handle your personal information safely?	Scale	Mean	SD
Trust in companies (TC)			
A company I am familiar with	1–5	2.80	1.121
A well-known company	1–5	2.96	1.169
An unknown company (removed) (reversed)	1–5	3.24	0.949

How concerned are you about the following risks in relation to your personal data?	Scale	Mean	SD
Data tracking concerns (DT)			
Companies possess information about me that I consider private	1–5	1.86	0.905
My personal information is used without my knowledge	1–5	1.67	0.897
My online personal data are used to send me commercial offers	1–5	1.64	0.897
My behavior and activities can be monitored online	1–5	1.92	0.983
My identity is reconstructed using personal data from various sources	1–5	1.79	0.952
My personal data are shared with third parties without my agreement	1–5	1.64	0.897

How concerned are you about the following risks in relation to your personal data?	Scale	Mean	SD
Identity damage concerns (ID)			
My reputation may be damaged by online personal information	1–5	2.11	1.068
My personal safety may be at risk due to online personal information	1–5	2.05	1.073
My identity is at risk of theft online	1–5	1.72	0.896
My views and behavior may be misrepresented based on online personal information	1–5	2.01	0.979
I may be victim of financial fraud online	1–5	1.74	0.947

How likely are you to provide personal data for the following reasons?	Scale	Mean	SD
Utilitarian rewards (UR)			
To save time (not to type information several times for instance)	1–5	3.32	1.219
To benefit from a better service (e.g., education, health, etc.)	1–5	3.55	1.049
To benefit from personalized commercial offers	1–5	2.96	1.173
To receive gifts or samples	1–5	3.07	1.195
To receive money or price reductions	1–5	3.24	1.183
To log on securely onto a system (removed)	1–5	3.94	1.151

How likely are you to provide personal data for the following reasons?	Scale	Mean	SD
Hedonic rewards (HR)			
To receive valuable information	1–5	3.57	1.038
To enjoy, to take pleasure	1–5	3.24	1.096

Appendix 3 (*Continued*)

How likely are you to provide personal data for the following reasons?	Scale	Mean	SD
To take a good action, to help	1–5	3.30	1.086
To connect with others	1–5	3.50	1.111

I usually protect my personal data and identity in the following ways	Scale	Mean	SD
Technical protection (TP)			
Scan data with anti-spyware	1–4	3.09	0.997
Update virus protection	1–4	3.26	0.929
Install operating system patches	1–4	2.54	1.172
Use tools limiting the collection of personal data from my computer (e.g., firewall, cookie filtering)	1–4	2.94	1.018
Erase cookies	1–4	2.68	1.022
Use tools and strategies to limit unwanted email	1–4	2.92	0.977
Check that the transaction is protected or the site has a safety badge before I enter valuable personal data	1–4	3.05	0.986

General caution (GC)	Scale	Mean	SD
Adapt my personal data so that no linking between profiles is possible	1–4	2.24	1.019
Read the privacy policy of websites	1–4	2.26	0.915
Change the security settings of my browser to increase privacy (removed)	1–4	2.43	1.002

Withholding (WI)	Scale	Mean	SD
Give a minimum of information	1–4	2.76	0.823
Do not give personal details	1–4	2.38	0.781

What do you think are the efficient ways to protect your identity and privacy?	Scale	Mean	SD
Regulatory preferences (RP)			
Give users more direct control of their own identity data	1–4	2.92	0.756
Allocate more resources to monitoring and enforcing existing regulations	1–4	2.98	0.757
Require that service providers take greater care of their customers' identity	1–4	3.21	0.803
Provide formal education on safe identity management	1–4	3.00	0.788
Set up clear guidelines for safe identity management, online and offline	1–4	3.14	0.758

Do you do the following activities on the Internet? (Tick all that apply.)	Percentage ticked
Internet activities (used in post hoc analysis)	
Check email (B)[9]	80%
Instant messaging (A)	65%
Participate in chat rooms, newsgroups or an online discussion forum (A)	30%
Use a search engine to find information (B)	93%
Use websites (flicker, YouTube, etc.) to share pictures, videos, movies etc. (A)	50%
Manage your profile on a social networking site such as YouTube, MySpace, or Facebook (A)	54%
Keep a web-log (or a blog) (A)	8%
Use peer-to-peer software to exchange movies, music, etc. (A)	17%

Appendix 4. Outer loadings

Item	Loading	St Dev.	T Statistics
PRP1	0.763	0.021	36.943
PRP2	0.833	0.015	54.011
PRP3	0.881	0.010	84.579
PRP4	0.818	0.016	52.151
PRP5	0.877	0.011	80.779
PRP6	0.866	0.011	75.382
TR1	0.910	0.008	114.122
TR2	0.951	0.005	200.831
TR3	0.931	0.008	122.682
TC1	0.952	0.005	182.823
TC2	0.951	0.006	171.642
DTC1	0.815	0.018	44.339
DTC2	0.898	0.009	100.680
DTC3	0.898	0.008	107.645
DTC4	0.812	0.018	45.119
DTC5	0.802	0.020	40.685
DTC6	0.857	0.013	66.711

[9] (B) denotes a "Basic" task; (A) denotes an "Advanced" task.

Appendix 4 (*Continued*)

Item	Loading	St Dev.	T Statistics
IDC1	0.833	0.014	60.081
IDC2	0.842	0.014	59.371
IDC3	0.894	0.009	103.944
IDC4	0.864	0.012	74.449
IDC5	0.856	0.014	62.269
UR1	0.749	0.019	39.318
UR2	0.739	0.019	39.934
UR3	0.797	0.014	56.409
UR4	0.837	0.012	72.418
UR5	0.824	0.014	59.206
HR1	0.844	0.013	62.545
HR2	0.902	0.008	109.551
HR3	0.886	0.009	99.141
HR4	0.756	0.020	37.604
TP1	0.830	0.012	68.777
TP2	0.827	0.013	65.624
TP3	0.705	0.017	40.510
TP4	0.726	0.018	39.480
TP5	0.772	0.015	50.082
TP6	0.746	0.019	40.158
TP7	0.822	0.013	62.934
GC1	0.871	0.011	81.879
GC2	0.905	0.006	156.396
W1	0.829	0.023	36.348
W2	0.809	0.024	33.393
RP1	0.814	0.020	41.033
RP2	0.794	0.019	41.652
RP3	0.612	0.041	14.881
RP4	0.782	0.020	39.361
RP5	0.762	0.023	32.919

Appendix 5. Loadings and Cross-Loadings

		Regulatory knowledge	Perceived regulatory protection	Trust in regulators	Trust in companies	Data tracking risks	Identity damage risks	Utilitarian rewards	Hedonic rewards	Technical protection	General caution	Withholding	Regulatory preferences
Regulatory knowledge	RK	1.000	0.071	−0.038	−0.044	0.130	0.087	−0.056	0.009	0.321	0.216	0.144	0.048
Perceived regulatory protection	PRP1	0.170	0.763	0.317	0.279	−0.172	−0.165	0.204	0.202	0.081	0.029	−0.069	0.037
	PRP2	0.055	0.833	0.327	0.271	−0.278	−0.248	0.241	0.196	−0.088	0.019	−0.106	−0.052
	PRP3	0.031	0.881	0.427	0.296	−0.289	−0.240	0.252	0.214	−0.114	−0.015	−0.112	−0.052
	PRP4	0.069	0.818	0.319	0.287	−0.239	−0.175	0.270	0.238	−0.044	0.073	−0.091	0.011
	PRP5	0.035	0.877	0.418	0.290	−0.292	−0.238	0.272	0.230	−0.104	0.033	−0.118	−0.039
	PRP6	0.025	0.866	0.434	0.299	−0.282	−0.214	0.261	0.241	−0.107	0.037	−0.080	−0.020
Trust in regulators	TR1	−0.048	0.403	0.910	0.522	−0.241	−0.184	0.365	0.305	−0.208	−0.121	−0.194	0.027
	TR2	−0.043	0.445	0.951	0.493	−0.202	−0.138	0.344	0.298	−0.194	−0.094	−0.196	0.069
	TR3	−0.013	0.405	0.931	0.462	−0.215	−0.158	0.310	0.313	−0.174	−0.083	−0.196	0.054
Trust in companies	TC1	−0.048	0.340	0.511	0.952	−0.166	−0.119	0.391	0.356	−0.141	−0.129	−0.167	0.099
	TC2	−0.035	0.309	0.498	0.951	−0.153	−0.092	0.360	0.341	−0.113	−0.114	−0.108	0.100
Data tracking risks	DT1	0.076	−0.280	−0.225	−0.165	0.815	0.656	−0.109	−0.050	0.169	0.137	0.125	0.199
	DT2	0.144	−0.261	−0.188	−0.123	0.898	0.702	−0.090	−0.018	0.212	0.102	0.183	0.218
	DT3	0.139	−0.253	−0.174	−0.116	0.898	0.673	−0.108	−0.001	0.237	0.068	0.186	0.222
	DT4	0.080	−0.236	−0.214	−0.137	0.812	0.621	−0.118	−0.036	0.189	0.084	0.165	0.166
	DT5	0.094	−0.255	−0.176	−0.134	0.802	0.575	−0.178	−0.055	0.202	0.117	0.147	0.160
	DT6	0.125	−0.297	−0.222	−0.179	0.857	0.711	−0.125	−0.045	0.255	0.106	0.183	0.205
Identity damage risks	ID1	0.071	−0.218	−0.153	−0.130	0.660	0.833	−0.022	0.018	0.147	0.129	0.080	0.138
	ID2	0.030	−0.247	−0.161	−0.096	0.596	0.842	−0.016	0.020	0.147	0.121	0.078	0.101
	ID3	0.101	−0.250	−0.163	−0.090	0.725	0.894	−0.040	−0.010	0.211	0.092	0.160	0.201
	ID4	0.053	−0.166	−0.098	−0.085	0.617	0.864	0.021	0.024	0.115	0.133	0.079	0.160
	ID5	0.110	−0.216	−0.161	−0.078	0.721	0.856	−0.036	0.008	0.235	0.095	0.150	0.198
Utilitarian rewards	UR1	−0.047	0.225	0.294	0.274	−0.144	−0.064	0.749	0.617	−0.229	−0.176	−0.207	0.141
	UR2	−0.006	0.230	0.340	0.350	−0.062	−0.015	0.739	0.715	−0.156	−0.145	−0.172	0.207
	UR3	−0.046	0.228	0.276	0.293	−0.145	−0.022	0.797	0.580	−0.201	−0.073	−0.267	0.046
	UR4	−0.083	0.259	0.279	0.308	−0.121	0.000	0.837	0.569	−0.205	−0.125	−0.241	0.036
	UR5	−0.043	0.234	0.249	0.329	−0.089	0.011	0.824	0.559	−0.162	−0.139	−0.175	0.047

Appendix 5 (*Continued*)

		Regulatory knowledge	Perceived regulatory protection	Trust in regulators	Trust in companies	Data tracking risks	Identity damage risks	Utilitarian rewards	Hedonic rewards	Technical protection	General caution	Withholding	Regulatory preferences
Hedonic rewards	HR1	0.021	0.227	0.300	0.340	−0.030	0.019	0.671	0.844	−0.159	−0.177	−0.189	0.188
	HR2	−0.002	0.217	0.250	0.290	−0.028	0.003	0.674	0.902	−0.204	−0.145	−0.241	0.124
	HR3	0.027	0.237	0.318	0.321	−0.057	−0.025	0.656	0.886	−0.150	−0.101	−0.217	0.179
	HR4	−0.019	0.207	0.243	0.292	−0.016	0.054	0.619	0.756	−0.157	−0.102	−0.244	0.125
Technical protection	TP1	0.224	−0.061	−0.163	−0.066	0.233	0.204	−0.169	−0.129	0.830	0.387	0.276	0.112
	TP2	0.238	−0.081	−0.162	−0.077	0.237	0.202	−0.168	−0.157	0.827	0.396	0.259	0.136
	TP3	0.232	−0.025	−0.108	−0.088	0.075	0.066	−0.119	−0.112	0.705	0.453	0.232	0.088
	TP4	0.211	−0.096	−0.171	−0.131	0.205	0.164	−0.198	−0.159	0.726	0.432	0.221	0.088
	TP5	0.276	−0.080	−0.154	−0.083	0.197	0.162	−0.195	−0.154	0.772	0.447	0.313	0.143
	TP6	0.290	−0.040	−0.163	−0.142	0.188	0.143	−0.219	−0.167	0.746	0.502	0.273	0.097
	TP7	0.273	−0.062	−0.197	−0.140	0.208	0.148	−0.238	−0.190	0.822	0.555	0.318	0.090
General caution	GC1	0.178	0.046	−0.103	−0.122	0.115	0.138	−0.130	−0.123	0.460	0.871	0.239	0.081
	GC2	0.203	0.014	−0.088	−0.106	0.100	0.100	−0.164	−0.151	0.570	0.905	0.278	0.070
Withholding	W1	0.123	−0.114	−0.172	−0.109	0.201	0.150	−0.198	−0.175	0.303	0.228	0.829	0.071
	W2	0.113	−0.073	−0.172	−0.129	0.117	0.060	−0.243	−0.255	0.269	0.252	0.809	0.008
Regulatory preferences	RP1	0.047	−0.061	0.045	0.070	0.224	0.166	−0.077	−0.137	0.176	0.087	0.072	0.814
	RP2	0.031	−0.040	0.024	0.047	0.194	0.152	−0.083	−0.141	0.095	0.079	0.034	0.794
	RP3	0.021	0.016	0.043	0.069	0.098	0.089	−0.134	−0.141	0.016	0.087	−0.001	0.612
	RP4	0.090	−0.010	0.039	0.110	0.193	0.152	−0.073	−0.146	0.140	0.028	0.034	0.782
	RP5	−0.019	0.009	0.055	0.103	0.147	0.142	−0.110	−0.126	0.074	0.043	0.039	0.762

References

[1] A. Acquisti, J. Grossklags, Privacy and rationality in individual decision making, IEEE Secur. Priv. 3, 2005, pp. 26–33.
[2] J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: a review and recommended two-step approach, Psychol. Bull. 103, 1988, pp. 411–423.
[3] J.S. Armstrong, T.S. Overton, Estimating non-response bias in mail surveys, J. Mark. Res. 14, 1977, pp. 396–402.
[4] J. Backhouse, R. Halperin, A survey on EU citizens' trust in ID systems and authorities, FIDIS J. 1, 2007.
[5] G. Bansal, F.M. Zahedi, D. Gefen, The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online, Decis. Support Syst. 49, 2010, pp. 138–150.
[6] F. Bélanger, R. Crossler, Privacy in the digital age: a review of information privacy research in information systems, MIS Q. 35, 2011, pp. 1017–1041.
[7] F. Bélanger, J.S. Hiller, W.J. Smith, Trustworthiness in electronic commerce: the role of privacy, security, and site attributes, J. Strateg. Inf. Syst. 11, 2002, pp. 245–270.
[8] C.J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Cornell University Press, 1992.
[9] T. Buchanan, C. Paine, A.N. Joinson, U.-D. Reips, Development of measures of online privacy concern and protection for use on the Internet, J. Am. Soc. Inf. Sci. Technol. 58, 2007, pp. 157–165.
[10] J. Carifio, R.J. Perla, Ten common misunderstandings, misconceptions, persistent myths and urban legends about Likert scales and Likert response formats and their antidotes, J. Soc. Sci. 3, 2007, pp. 106–116.
[11] L. Chang, A psychometric evaluation of 4-point and 6-point Likert-type scales in relation to reliability and validity, Appl. Psychol. Meas. 18, 1994, pp. 205–215.
[12] W.W. Chin, Issues and opinion on structural equation modeling, MIS Q. 22, 1998, pp. vii–xvi.
[13] W.W. Chin, The partial least squares approach to structural equation modeling, in: G.A. Marcoulides (Ed.), Modern Methods for Business Research, Lawrence Erlbaum Associates, Inc., 1998, pp. 295–336.
[14] 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, Inf. Syst. Res. 14, 2003, pp. 189–217.
[15] W.W. Chin, J.B. Thatcher, R.T. Wright, Assessing common method bias: problems with the ULMC technique, MIS Q. 36, 2012, pp. 1003–1020.
[16] P. Chwelos, I. Benbasat, A.S. Dexter, Research report: empirical test of an EDI adoption model, Inf. Syst. Res. 12, 2001, pp. 304–321.
[17] D.R. Compeau, C.A. Higgins, S. Huff, Social cognitive theory and individual reactions to computing technology: a longitudinal study, MIS Q. 23, 1999, pp. 145–158.
[18] Consumers-Union, Consumer reports poll: Americans extremely concerned about Internet privacy, September 25.
[19] M.J. Culnan, Consumer awareness of name removal procedures: implications for direct marketing, J. Direct Mark. 7, 1995, pp. 10–19.
[20] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation, Organ. Sci. 10, 1999, pp. 104–115.
[21] J. Dawes, Do data characteristics change according to the number of scale points used? An experiment using 5-point, 7-point, and 10-point scales Int. J. Mark. Res. 50, 2008, pp. 61–77.
[22] T. Dinev, M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti, Privacy calculus model in e-commerce – a study of Italy and the United States, Eur. J. Inf. Syst. 15, 2006, pp. 389–402.
[23] T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Inf. Syst. Res. 17, 2006, pp. 61–80.
[24] S. Dolnicar, Y. Jordaan, Protecting consumer privacy in the company's best interest, Australas. Mark. J. 14, 2006, pp. 39–61.
[25] C.J. Dommeyer, B.L. Gross, What consumers know and what they do: an investigation of consumer knowledge, awareness, and use of privacy protection strategies, J. Interact. Mark. 17, 2003, pp. 34–51.
[26] Equifax Inc., Equifax-Harris mid-decade consumer privacy survey 1995, 1995.
[27] D.H. Flaherty, Protecting Privacy in Surveillance Societies, University of North Carolina Press, 1989.
[28] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18, 1981, pp. 39–50.
[29] G. Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State, Hamish Hamilton, 2014.
[30] C. Guinot, M. Latreille, M. Tenenhaus, PLS path modeling and multiple table analysis: application to the cosmetic habits of women in Ile-de-France, Chemom. Intell. Lab. Syst. 58, 2001, pp. 247–259.
[31] J.F. Hair, C.M. Ringle, M. Sarstedt, PLS-SEM: indeed a silver bullet, J. Mark. Theory Pract. 19, 2011, pp. 139–151.
[32] Harris Interactive, Mobile privacy: A user's perspective, Truste.
[33] E.C. Hirschman, M.B. Holbrook, Hedonic consumption: emerging concepts, methods and propositions, J. Mark. 46, 1982, pp. 92–101.
[34] G.H. Hofstede, Culture's Consequences, International Differences in Work-Related Styles, Sage, 1980.
[35] M.B. Holbrook, E.C. Hirschman, The experiential aspects of consumption: consumer fantasies, feelings, and fun, J. Consum. Res. 9, 1982, pp. 132–140.
[36] J. Hsieh, A. Rai, M. Keil, Understanding digital inequality: comparing continued user behavioral models of the socio-economically advantaged and disadvantaged, MIS Q. 32, 2008, pp. 97–126.
[37] J. Jacoby, M.S. Matell, Three-point Likert scales are good enough, J. Mark. Res. 8, 1971, pp. 495–500.
[38] K.G. Joreskog, H. Wold, The ML and PLS techniques for modeling with latent variables: historical and comparative aspects, in: H. Wold, K.G. Joreskog (Eds.), Systems Under Indirect Observation, Part I, North-Holland, 1982, pp. 263–270.
[39] J. Kanter, A nudge on digital privacy law from EU official, The New York Times ed, April 1, 2014.
[40] B. Lee, Users' perspective on regulation to protect privacy on the web, Int. Inf. Libr. Rev. 32, 2000, pp. 379–402.
[41] Y. Li, Empirical studies on online information privacy concerns: literature review and an integrative framework, Commun. Assoc. Inf. Syst. 28, 2011, pp. 453–496.
[42] H. Liang, N. Saraf, Q. Hu, Y. Xue, Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management, MIS Q. 31, 2007, pp. 59–87.
[43] J.B. Lohmoller, Latent variables path modeling with partial least squares, Physica 1989.
[44] S. Lohr, The privacy paradox, a challenge for business, The New York Times ed, New York, June 12, 2014.
[45] M. Lwin, J. Wirtz, J.D. Williams, Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective, J. Acad. Mark. Sci. 35, 2007, pp. 572–585.

[46] R.O. Mason, Four ethical issues of the information age, MIS Q. 10, 1986, pp. 5–12.
[47] R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust, Acad. Manag. Rev. 20, 1995, pp. 709–734.
[48] D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: an integrative typology, Inf. Syst. Res. 13, 2002, pp. 334–359.
[49] S.J. Milberg, H.J. Smith, S.J. Burke, Information privacy: corporate management and national regulation, Organ. Sci. 11, 2000, pp. 35–57.
[50] G.R. Milne, A.J. Rohm, S. Bahl, Consumers' protection of online privacy and identity, J. Consum. Aff. 38, 2004, pp. 217–232.
[51] C.L. Miltgen, D. Peyrat-Guillard, Cultural and generational influences on privacy concerns: a qualitative study in seven European countries, Eur. J. Inf. Syst. 23, 2014, pp. 103–125.
[52] C.L. Miltgen, A. Popovic, T. Oliveira, Determinants of end-user acceptance of biometrics: integrating the "Big 3" of technology acceptance with privacy context, Decis. Support Syst. 56, 2013, pp. 103–114.
[53] A.N. Mishra, R. Agarwal, Technological frames, organizational capabilities, and IT use: a empirical investigation of electronic procurement, Inf. Syst. Res. 21, 2010, pp. 249–270.
[54] R. Noonan, H. Wold, Evaluating school systems using partial least squares, Eval. Educ. 7, 1983, pp. 219–364.
[55] P.A. Norberg, D.R. Horne, D.A. Horne, The privacy paradox: personal information disclosure intentions versus behaviors, J. Consum. Aff. 41, 2007, pp. 100–126.
[56] G.J. Nowak, J. Phelps, Direct marketing and the use of individual-level consumer information: determining how and when 'privacy' matters, J. Direct Mark. 9, 1995, pp. 46–60.
[57] G.J. Nowak, J. Phelps, Understanding privacy concerns: an assessment of consumers information-related knowledge and beliefs, J. Direct Mark. 6, 1992, pp. 28–39.
[58] S. Okazaki, H. Li, M. Hirose, Consumer privacy concerns and preference for degree of regulatory control: a study of mobile advertising in Japan, J. Advert. 38, 2009, pp. 63–77.
[59] C. Park, M. Keil, J.W. Kim, The effect of it failure impact and personal morality on IT project exporting behaviors, IEEE Trans. Eng. Manag. 56, 2009, pp. 45–60.
[60] Y.J. Park, S.W. Campbell, N. Kwak, Affect, cognition, and reward: predictors of privacy protection online, Comput. Hum. Behav. 28, 2012, pp. 1019–1027.
[61] P. Pavlou, State of the information privacy literature: where we are now and where should we go? MIS Q. 35, 2011, pp. 977–988.
[62] P. Podsakoff, S. MacKenzie, J. Lee, N. Podsakoff, Common method bias in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88, 2003, pp. 879–903.
[63] C. Posey, P.B. Lowry, L.P. Robert, T.S. Ellis, Proposing the online community self-disclosure model: the case of working professionals in France and the UK who use online communities, Eur. J. Inf. Syst. 19, 2010, pp. 181–195.
[64] J.L. Rasmussen, Analysis of Likert-scale data: a reinterpretation of Gregoire and Driver, Psychol. Bull. 105, 1989, pp. 167–170.
[65] C.M. Ringle, S. Wende, A. Will, SmartPLS 2.0 m3.
[66] F. Robinson, S. Schechner, A. Mizroch, EU orders Google to let users erase past, The Wall Street Journal ed, May 13, 2014.
[67] F.D. Schoorman, R.C. Mayer, J.H. Davis, An integrative model of organizational trust: past, present, and future, Acad. Manag. Rev. 32, 2007, pp. 344–354.
[68] N. Singer, Data protection laws, an ocean apart, The New York Times ed, February 2, 2013.
[69] H.J. Smith, Information privacy and marketing: what the US should (and shouldn't) learn from Europe, Calif. Manag. Rev. 43, 2001, pp. 8–33.
[70] H.J. Smith, Managing Privacy: Information Technology and Corporate America, University of North Carolina Press, 1994.
[71] H.J. Smith, T. Dinev, H. Xu, Information privacy research: an interdisciplinary review, MIS Q. 35, 2011, pp. 989–1015.
[72] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. 20, 1996, pp. 167–196.
[73] J. Smith, Privacy policies and practices: inside the organizational maze, Commun. ACM 36, 1993, pp. 105–122.
[74] M. Sobel, Asymptotic confidence intervals for indirect effects on structural equation models, Sociol. Methodol. 13, 1982, pp. 290–312.
[75] D.W. Straub, Validating instruments in MIS research, MIS Q. 13, 1989, pp. 147–169.
[76] D.W. Straub, M.-C. Boudreau, D. Gefen, Validation guidelines for IS positivist research, Commun. Assoc. Inf. Syst. 13, 2004, pp. 380–427.
[77] M. Tenenhaus, V.E. Vinzi, Y.-M. Chatelin, C. Lauro, PLS path modeling, Comput. Stat. Data Anal. 48, 2005, pp. 159–205.
[78] The Wall Street Journal, The morning risk report: EU ruling on Google is a 'game changer,' attorney says, The Wall Street Journal ed, May 14, 2014.
[79] J. Turow, M. Hennessy, A. Bleakley, Consumers' understanding of privacy rules in the marketplace, J. Consum. Aff. 42, 2008, pp. 411–424.
[80] H. Van der Heijden, User acceptance of hedonic information systems, MIS Q. 28, 2004, pp. 695–704.
[81] A. Vance, C. Elie-Dit-Cosaque, D.W. Straub, Examining trust in information technology artifacts: the effects of system quality and culture, J. Manag. Inf. Syst. 24, 2008, pp. 73–100.
[82] J. Wirtz, M. Lwin, J.D. Williams, Causes and consequences of consumer online privacy concern, Int. J. Serv. Ind. Manag. 18, 2007, pp. 326–348.
[83] H. Wold, Soft modeling: the basic design and some extensions, in: K.G. Joreskog, H. Wold (Eds.), Systems Under Indirect Observation: Part I, North-Holland, 1982, pp. 1–54.
[84] H. Xu, T. Dinev, H.J. Smith, P. Hart, Information privacy concerns: linking individual perceptions with institutional privacy assurances, J. Assoc. Inf. Syst. 12, 2011, pp. 798–824.
[85] H. Xu, H.H. Teo, B.C.Y. Tan, J. Agarwal, Research note – effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Inf. Syst. Res. 23, 2012, pp. 1342–1363.
[86] S. Youn, Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents, J. Consum. Aff. 43, 2009, pp. 389–418.
[87] S. Youn, Parental influence and teens' attitude toward online privacy protection, J. Consum. Aff. 42, 2008, pp. 362–388.

Caroline Lancelot Miltgen is Associate Professor in Marketing at Audencia School of Management. Her research interests include information privacy, e-commerce and public policy, social media, digital services and technology acceptance. Prof. Lancelot Miltgen is the author of several academic articles and book chapters in the field of Information Systems and Marketing. She recently published an article on Biometrics acceptance in Decision Support Systems and another one on Cultural and generational influences on privacy concerns in the European Journal of Information Systems. She was the leader and principal investigator of two research contracts for the European Commission on 'Privacy and electronic identification systems' (2007) and on 'Personal data management' (2009).

H. Jeff Smith is the George and Mildred Panuska Professor in Business in the Farmer School of Business at Miami University in Oxford, Ohio. His research focuses on ethical, societal, and regulatory issues associated with strategic uses of information technology. His research also examines organizational impediments to successful implementation of information technology applications. His research has appeared in California Management Review, Communications of the ACM, Harvard Business Review, MIS Quarterly, MIT Sloan Management Review, Organization Science, and in other journals. He serves as a Senior Editor of Decision Sciences. He served on the editorial board of MIS Quarterly from 2003–2006 and as Chair of the Department of Decision Sciences and Management Information Systems at Miami University (Ohio) from July 2006 until July 2011. He holds B.S. degrees in computer science and math from North Carolina State University; an M.B.A. degree from the University of North Carolina in Chapel Hill; and a D.B.A. degree from Harvard University. He worked for the International Business Machines (IBM) Corporation for several years in the area of software development.