Exploring information privacy regulation, risks, trust, and behavior

Caroline Lancelot Miltgen, H. Jeff Smith

Caroline Lancelot Miltgen
Audencia School of Management, 8 route de la Jonelière, BP 31222, 44312 Nantes Cedex 3, France

H. Jeff Smith
Department of Information Systems and Analytics, Farmer School of Business, Miami University, Oxford, OH, USA

EXPLORING INFORMATION PRIVACY REGULATION, RISKS, TRUST, AND BEHAVIOR

Abstract

Over the past few decades, governments worldwide have grappled with their approaches to regulating issues associated with information privacy. However, research into 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 associated with 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.

Keywords

Information privacy, protection, regulation, trust, risk, rewards

EXPLORING INFORMATION PRIVACY REGULATION, RISKS, TRUST, AND BEHAVIOR

1. Introduction

Beginning in the 1970s, attention worldwide has been focused on information privacy. By 1986, privacy had been denoted 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 1,000 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 for 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 individual on the Web when those individuals request it [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 being devoted to privacy issues and the tensions associated therewith, there has been very little research associated with that relationship at either a corporate or an individual level.

At the corporate level, one must look back almost 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 have considered a comprehensive model that addresses the complexity of individuals' decision-making models.

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 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 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 go further by identifying components of the shared space 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, and privacy risk concerns; two outcome variables (protection behavior and regulatory preferences); and direct and moderating effects associated with perceived rewards. It stands as the first offering to look across that spectrum of relationships by considering some selected variables within each domain associated with privacy regulation.

Third, for four constructs that had been given only limited attention in prior research--regulatory knowledge, privacy risk concerns, regulatory preferences, and perceived rewards—

this study provides a starting set of measurement scales that can be used by future researchers as they delve more deeply into these constructs 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 associated therewith. We follow this with a discussion of the study's method, and we detail our findings. We then discuss implications of this study, not only for researchers but also for management and regulation.

2. Background

Our consideration 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 sometimes been included. The manner in which regulatory attributes result in actions taken by individuals [25, 45, 82] and in 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 towards a more cohesive knowledge base, we consider a model that looks across the framework called "APCO" (antecedents – privacy concerns – outcomes) by Smith et al. [71] by including both 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 associated with regulation (trust), and a construct (perceived rewards) that has been argued and shown in other privacy-related research studies to be of some importance in individuals' decision-making (e.g., [1, 23, 86]) but that has been overlooked too in the regulation studies. Our objective in testing this model is to provide a more cohesive view of privacy regulation findings and to also extend those findings by incorporating what we believe to be some of the most promising constructs from the broader privacy research domain. We turn now to the specific model that is addressed in this study.

TABLE 1[1]
PREVIOUS STUDIES – GOVERNMENTAL REGULATION AND OUTCOMES (INDIVIDUAL LEVEL)

Article	Sample	Antecedents[2]	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, Wirtz, and Williams [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, Smith, and Burke [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, Li, and Hirose [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, Hennessy, and Bleakley [79]	1,500 adults in telephone survey (random dial sample)	None	Level of knowledge of privacy rules	Gender, age, race/ethnicity, education, family income, parental status
Wirtz, Lwin, and Williams [82]	182 online subjects (recruited from commercial database)	Business policy, governmental regulation	User intentions (self-reported)	Privacy concerns
Xu, Teo, Tan, and Agarwal [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

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

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

3. Model development

As can be seen in Figure 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 but also on some other studies that have examined subordinate portions of the model (even if they did not consider the regulatory constructs) or that provide useful theoretical insights that may extrapolate to the immediate model. In addition, in some cases, we rely on our own argumentation to defend some hypotheses. We do not claim our model to be an exhaustive one, given the paucity of theoretical development in this research domain (see Table 1) and the constraints associated with data collection. Rather, we have attempted 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.

FIGURE 1
RESEARCH MODEL

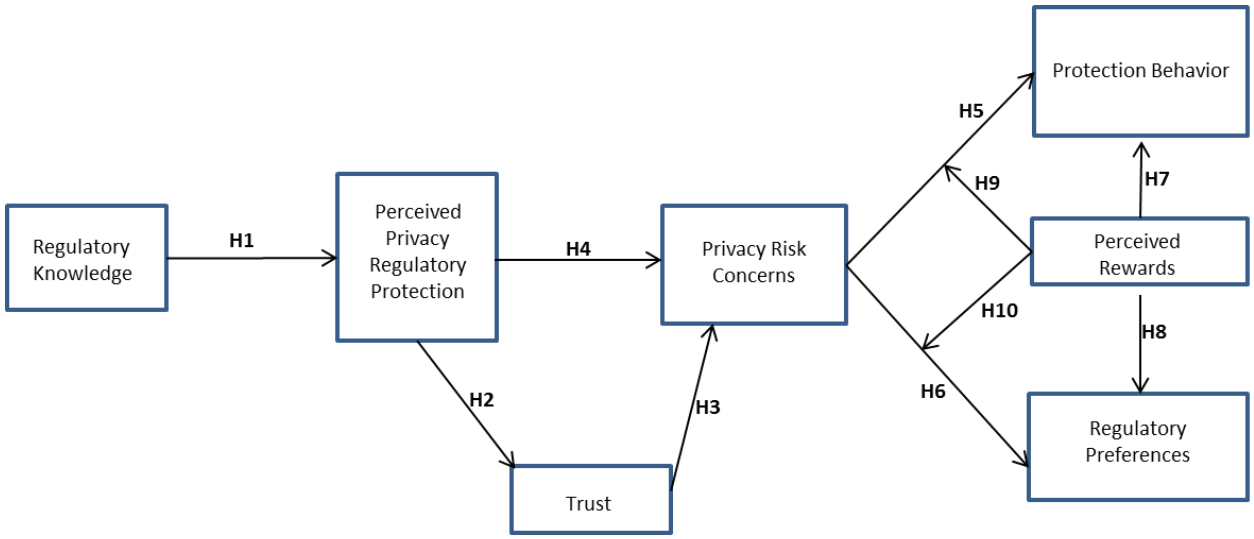


TABLE 2
HYPOTHESES

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.

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] revolved around *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 being 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]) did not consider such a relationship in 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:

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 associated with privacy. However, its specific relationship to other privacy-related constructs has not been consistent across studies, with trust serving variously as an antecedent, outcome, mediator, or moderator. In this study, for reasons to be discussed 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 embraced in our study is what has been called "impersonal trust" [20] and that has been explored by McKnight, Choudhury, and Kacmar [48] and considered in a complex research model by Bansal, Zahedi, and Gefen [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 embraced in this study is more complex: individuals could have a high level of trust in their government and/or a commercial entity, regardless of whether their own government provides protection in the form of regulation. In fact, it is this very 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. relies greatly on this approach [8, 69].

However, although such a model can be observed to be in use, we argue that it is not emotionally embraced by individuals 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:

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," since individuals' concerns about risks are likely the most salient attribute in a regulatory context.

We rely on the models studied by Bélanger, Hiller, and Smith [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 (and this could 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, since (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, Wirtz, and Williams [45] used power-relationship theory from sociology and social psychology to develop a model explaining individuals' perceptions and responses associated with 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] explain 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 findings, we propose:

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 topics in information privacy, 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 adoption of new technologies that protect privacy or challenge it [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 usually 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 by individual and context [71]. Thus, while acknowledging that some contradictions to the main body of findings do exist, we propose:

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), there are relatively few studies that consider the relationship between privacy risk concerns and regulatory preferences, which can be defined as an individual's preferences regarding the degree of regulatory control in his or her country to enforce user control of privacy. We note only two

studies that offer substantive guidance regarding this relationship. Okazaki, Li, and Hirose [58] found that individuals with higher concerns about risks in using mobile advertising applications prefer stricter regulatory controls to be enforced by the government. Earlier, Milberg, Smith, and Burke [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 about 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 own 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 usually view costs (including risks) and rewards (in most ways, synonymous with "benefits") as being directly juxtaposed against one another in a rational calculation.

To the extent that individuals do engage in a cognitive assessment of the tradeoff between costs and benefits in making privacy-related behavioral decisions, it stands to reason that the more individuals believe they will gain, the more they 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 could manifest itself in protection behavior and/or in different preferences for regulatory protection. Hence, we propose:

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 had considered only direct assessments of rewards and costs, a recent study [60] has 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 in 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 18-25 years old have distinctive online habits and make up 11 to 16% of the European population, this group is an important object of study in itself. Moreover, some of these young people will become key decision-makers in information technology (IT), and this generation as a whole will confront privacy-related issues to a degree their parents' generation will not. Therefore, it is vital to study young people in order to gain knowledge of how these issues are perceived and what are 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 United States samples [6], and the mix of student and consumer/professional samples varies by topic area [6]. Pavlou [61] notes 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. 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 to the survey were emailed to 140,476 UK young people,[3] selected through a database of European internet users managed by a French interactive marketing company, 1000mercis, through its fidelity program. 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 embraced 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 fully completed questionnaires[4] from UK respondents 18 to 25 years old.

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 ones (first quartile) with respect to age, gender and almost all of the constructs used in this 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. However, the *directionality* of those differences was inconsistent with what would have been observed had there been a non-response bias (that is, had early/late responders perceived more/less regulatory protection, consequently 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.

[3] The invitations were sent to individuals who were from 15 to 25 years old. In this study, we have omitted those respondents who were 15 to 17 years old.
[4] Only the participants who answered the entire survey have been 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%

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 that the use of multiple items be limited so as to shorten the survey, and that specific Likert scales be used for many items.[5] As a result, we were not always able to include all the survey items we would have liked.

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

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

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) figured the level of 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 taken from a previous EC survey on citizens' trust in ID systems and authorities [4].

The items measuring trust were developed taking into account both the digital environment and the specific focus of this study along with the previous literature on trust. We considered two different targets of trust, both the commercial entities with which any user can be in relation 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 already 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 kinds 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 show that people are significantly concerned about 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 used to identify the importance of two kinds of privacy risks that were identified in previous literature and confirmed through a preliminary exploratory study.

One deals with personal data handling mainly related to "data tracking" (DT) and the second with identity and financial fraud, which will be referred to "identity damage" (ID). Five and six items adapted from previous literature and the preliminary study form the privacy risk concerns scale used in the study, respectively referring to the data tracking and the identity damage concerns dimensions.

Protection behavior (PB) is a second-order construct distinguishing different forms of personal data protection strategies. Previous literature is rather inconclusive regarding the different dimensions that should be differentiated in this respect. Some authors differentiate social and technical protection (e.g. [60]), while others consider active versus passive protection (e.g. [24]). In most cases, studies include both technical protection and some other forms of protection. We embraced this dichotomy in developing our scale. Like Buchanan et al. [9], we considered "technical protection" (TP) and "general caution" (GC) as two important dimensions of protection to which we added a "withholding" (WI) dimension (called "refrain" by Youn [86]). We adapted from those previous scales a set of twelve (seven plus three plus two, respectively) 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 any user could have 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 could be taken by a government 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 measuring 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 distinguish two kinds of rewards – utilitarian and hedonic – that the user can expect in exchange for his/her personal data. 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 coupons) versus those which aim to provide self-fulfilling value to the user (hedonic rewards such as connecting with friends). Five plus four items representing utilitarian (UR) versus hedonic rewards (HR), respectively, 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
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 kind 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 on its 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 of 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

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[6] 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 are focusing on predicting the users' protection behavior and their 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), so 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 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.

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

(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 viewed as reflective indicators for these second-order latent variables[7].

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.[8]

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.[9] The first approach – which is increasingly in dispute [63, Appendix] but still widely reported (e.g. [36, 53, 59, 81]) - employed Harman's single-factor test [62]. All the variables were loaded into 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

[7] The loadings of the first order factors on the second-order factors were as follows: for trust: trust in companies (.812) and trust in regulators (.925); for privacy risk concerns: data tracking (.953) and identity damage (.931); for perceived rewards: utilitarian (.946) and hedonic (.937); for protection behavior: technical protection (.962), caution (.745) and withholding (.505).

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

[9] Following Chin et al.'s [15] recent advice, we did not embrace the approach of Liang et al. [42].

factor solution, or (2) one general factor accounts for the majority of the covariance in the variables [62]. Neither 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 around 0.70 while that by the method factor was around 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 .60 - .70 are often considered acceptable if the loadings of other items within the same construct are high [12, 13]. Thus, we have 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 .50, indicating good convergent validity for the measurement model [28]. For sufficient discriminant validity to be present, items should load

more strongly on 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 on their own latent constructs than on any other latent constructs (cross-loadings). In addition, the AVE square roots are larger than correlations among constructs (Table 6). Therefore, discriminant validity is achieved.

TABLE 5
STATISTICS FOR CONSTRUCTS

	Number of items	Mean	Std Dev.	CR	AVE	R Square	Cronbach Alpha
RK	1	2.75	.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	.90	0.951	0.906	0.661	0.893
DT	6	3.20	.79	0.939	0.719	0.908	0.921
ID	5	1.74	.85	0.933	0.736	0.867	0.910
UR	5	3.22	.92	0.892	0.624	0.894	0.849
HR	4	3.40	.91	0.911	0.721	0.877	0.869
TP	7	2.93	.78	0.914	0.604	0.925	0.890
GC	2	2.33	.90	0.882	0.788	0.555	0.733
WI	2	2.57	.66	0.803	0.670	0.255	0.509
RP	5	3.05	.58	0.869	0.572	0.086	0.810

LEGEND: **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 AVE'S

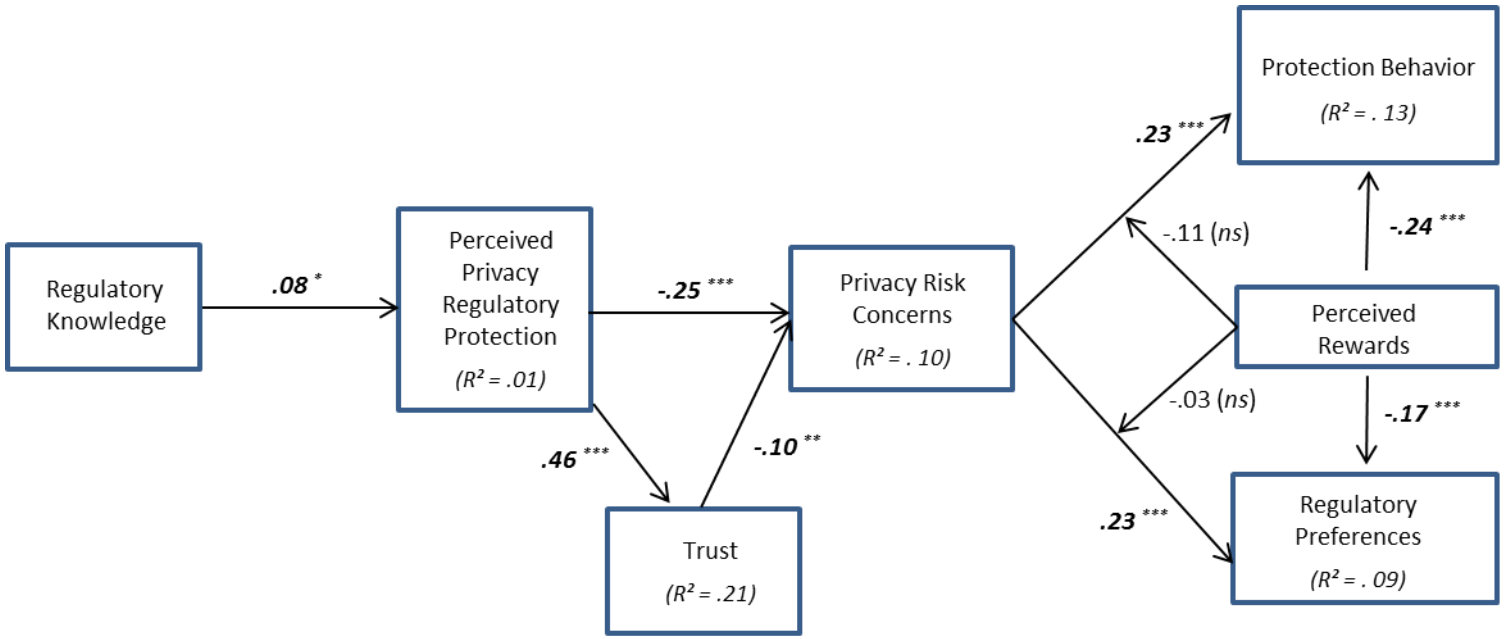
	RK	PRP	TR	TC	DT	ID	UR	HR	PB	GC	WI	RP
RK	**1.000**											
PRP	0.072	**0.841**										
TR	-0.038	0.449	**0.931**									
TC	-0.044	0.341	0.530	**0.952**								
DT	0.130	-0.311	-0.235	-0.167	**0.848**							
ID	0.087	-0.256	-0.172	-0.111	0.776	**0.858**						
UR	-0.056	0.298	0.365	0.395	-0.141	-0.022	**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**

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

LEGEND: * $p < .05$
** $p < .01$
*** $p < .001$

FIGURE 2
RESULTS MODEL



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 of 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 Figure 2. Eight of the ten hypotheses are validated, and the model explains 10% of privacy risk concerns, 21.3% of trust, 12.9% of protection behavior, and 8.6% of regulatory preferences. Regarding these percentages, it will be recalled that we do not claim our model to be an exhaustive one, given the paucity of theoretical development in this research domain. As will be discussed in Section 6.2.2, future studies could embrace more complex models with additional constructs.

We supposed that perceived privacy regulatory protection would be negatively influenced by awareness of privacy regulation, and it proved to be true (b = 0.075, t = 2.132), therefore 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), therefore supporting H2. Trust itself was 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 and did influence them this way (b = -0.253, t = 6.418), therefore supporting H4. Privacy risk concerns were in turn predicted to influence both dependent variables. We found that privacy risk concerns indeed influenced both

protection behavior (b = 0.227, t = 6.063) and regulatory preferences (b = 0.229, t = 6.379), therefore supporting H5 and H6. The 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), meaning that the more the person is expecting rewards in exchange of his/her data, the less (s)he tends to embrace any specific self-protection behavior, therefore validating H7. This result supports the privacy calculus process—that is, if the individual perceives 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), therefore validating H8. The more the individual is expecting rewards in exchange of his/her data, the less (s)he is looking for some help from the government to give him/her control of his/her data. We finally 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, 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 x b* is significant (i.e., if H_0: a x 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. Results appear in Table 8.

We find 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 confirm 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 confirm 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 could also influence 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 in which each respondent reporting engaging online from a list of eight classical activities (e.g., instant messaging, sharing pictures or videos, keeping a blog, checking emails). The two groups are called respectively "Basic" (people engaging in only classical online activities such as checking emails and using a search engine) and "Advanced" (people embracing 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. Results are shown in Table 9.

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 x b)	0.033	-0.019	-0.040	-0.068	-0.061
TOTAL EFFECT (a x 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

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 insignificant for Basic individuals. We therefore find 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, but is specific to the links between perceived regulatory protection and trust and between rewards and regulatory preferences.

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	ns
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	ns
Perceived Regulatory Protection -> Privacy Risk Concerns	-0.228	-0.323	-0.350	-0.449	-0.102	-0.230	0.096	0.128	ns
Privacy Risk Concerns -> Protection Behavior	0.284	0.173	0.172	0.051	0.367	0.285	0.112	0.083	ns
Privacy Risk Concerns -> Regulatory Preferences	0.158	0.152	0.036	0.060	0.262	0.274	0.006	0.475	ns
Perceived Rewards -> Protection Behavior	-0.238	-0.252	-0.310	-0.335	-0.074	-0.082	0.014	0.434	ns
Perceived Rewards -> Regulatory Preferences	-0.248	-0.072	-0.043	0.146	-0.313	-0.110	0.176	**0.033**	< 5%
Privacy Risk Concerns x Perceived Rewards-> Protection Behavior	-0.176	-0.129	-0.446	-0.481	-0.219	-0.216	0.047	NA	ns
Privacy Risk Concerns x Perceived Rewards-> Regulatory Preferences	0.159	-0.307	0.238	-0.547	0.438	0.490	-0.148	NA	ns

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 had only been considered separately in previous research [25, 40, 45, 49, 58, 79, 82, 85]. These studies had, independently, identified some variables and relationships that may explain a number of perceptions, attitudes, and behavior associated with privacy regulation. In this paper, we have looked across these articles to identify components of the shared space 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, and privacy risk concerns; two outcome variables (protection behavior and regulatory preferences); and direct and moderating effects associated with perceived rewards. Although our model does not provide an exhaustive test of all antecedents, mediators, and outcome variables [71], it does stand as the first offering to look across that spectrum of relationships by considering some selected variables within each domain associated with privacy regulation.

Third, for four constructs that had been given only limited attention in prior research--regulatory knowledge, privacy risk concerns, regulatory preferences, and perceived rewards—this study provides a starting set of measurement scales that can be used by future researchers as they delve more deeply into these constructs 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 follow with 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 swamped 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 its importance 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 first highlight some limitations of this study.

6.1 Limitations

While this study makes important contributions to the literature, we do note three areas that could 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 an ideal one in which to study 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.

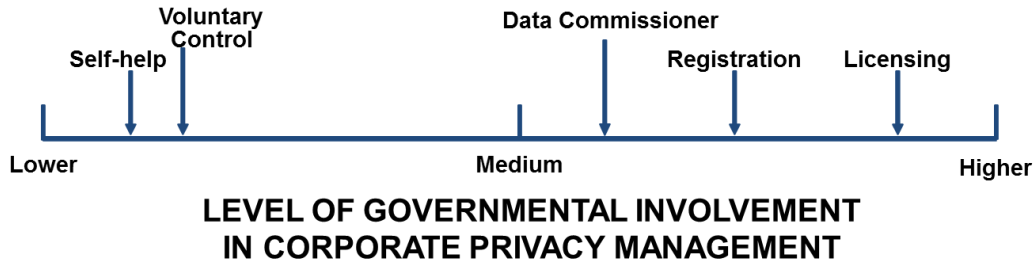
Strictly from the standpoint of generalizability, moving to a multi-country sample may not be required as numerous studies have drawn conclusions from single-country samples.

However, to the extent that cultural values within a given society may be impacting either the constructs or the relationships between them, it would be fruitful to examine those cultural impacts. This would be most readily achieved by comparison of 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, 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 are shown in Figure 3.

A multi-country sample, if constructed carefully, would allow an additional independent variable (regulatory model in a subject's country) to be tested for its association with subjects' perceptions of regulatory protection. It is generally assumed by regulators that the models on the right-hand side of Figure 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 Figure 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 this study – which would, of course, require a far larger sample drawn from multiple countries – would stand as a major contribution to the literature stream.

Figure 3 – Regulatory Models



1) The Self-Help model depends on data subjects' challenging recordkeeping 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* (usually 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 (usually, 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.

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 exposure from this limitation is modest, however, since 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 on our own, with 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 a complex one, 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 could be extended to deterring 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 could be expected to vary based on their treatment) would be measured, and their actual behavior could be observed and recorded. To the extent that differences in these behavioral variables were observed across treatment cells, one could 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 itself.

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 to these constructs (and to the relationships between them) deserves additional attention. Although some of our suppositions (direct effects on protection behavior and regulatory preferences) did find support, 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 the one 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 well benefit from including both direct and moderating effects of previous experiences in their data collection and modelling 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 considered governmental regulation and outcomes at the individual unit of analysis [25, 40, 45, 49, 58, 79, 82, 85]. Our own model (see Figure 1) does not purport to represent an exhaustive set of all the variables that had been considered previously, and some recent articles that review the broader domain of privacy research [6, 41, 71] reference a very large set of over two dozen antecedent constructs and about ten mediating or moderating variables, many of which could have an impact on behavior and regulatory preferences. It is obvious that numerous additional combinations of constructs could 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) could serve as antecedents to preferences for regulatory protections. Also note there could be additional moderating variables (in addition to perceived rewards, which we considered in H9 and H10) that could moderate those relationships.

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

6.2.3 Process model

As have almost 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 in a cross-sectional sense. 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 modelling could provide a rich understanding of the changes, over time, that occur in privacy-related relationships.

Generally speaking, process modelling 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. Most often, process modelling 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 modelling 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 could track changes in their behavior and preferences regarding regulation. If this were done along with a similar tracking process of changes in regulation at the national level (or within the EC, at the level of commission-level), rich insights might emerge. One could 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, but 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 to some degree these perceptions are cumulative – that is, they are not necessarily specific to one particular firm or organization – there is some room for managers to influence individuals in their behavioral calculations and, even, the extent to which they may demand regulatory protections.

Second, as was 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. Further, these perceptions manifest themselves in their protection behavior and, to some extent, in their 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 was shown above (in Figure 3), the UK's Registration model goes a great distance in providing 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 having to respond to individualistic behavioral choices by customers. Legal ambiguity is likely reduced via the more stringent regulatory models in Figure 3, even though this may mean that certain data collection and (re-)use practices are restricted.

7. Conclusion

With data collection increasing at a rapid rate in all industrialized societies, individuals' privacy-related behavior and their regulatory preferences are becoming subjects of increasing interest to marketers, policy-makers, 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 be seen not as an exhaustive test of a macro-model but, rather, 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.

REFERENCES

1. A. Acquisti, J. Grossklags, Privacy and rationality in individual decision making, IEEE Security & Privacy 3, 2005, pp. 26-33.
2. J.C. Anderson, D.W. Gerbing, Structural equation modeling in practice: A review and recommended two-step approach, Psychological Bulletin 103, 1988, pp. 411-423.
3. J.S. Armstrong, T.S. Overton, Estimating non-response bias in mail surveys, Journal of Marketing Research 14, 1977, pp. 396-402.
4. J. Backhouse, R. Halperin, A survey on EU citizens' trust in ID systems and authorities, Fidis Journal 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, Decision Support Systems 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 Quarterly 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, Journal of Strategic Information Systems 11, 2002, pp. 245-270.
8. C.J. Bennett, Regulating privacy: Data proection 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 privcy concern and protection for use on the internet, Journal of the American Society for Information Science and Technology 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, Journal of Social Sciences 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, Applied Psychological Measurement 18, 1994, pp. 205-215.
12. W.W. Chin, Issues and opinion on structural equation modeling, MIS Quarterly 22, 1998, pp. vii-xvi.
13. W.W. Chin, The partial least squares approach to structural equation modeling in Marcoulides, G.A. 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, Information Systems Research 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 Quarterly 36, 2012, pp. 1003-1020.
16. P. Chwelos, I. Benbasat, A.S. Dexter, Research report: Empirical test of an EDI adoption model, Information systems research 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 Quarterly 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, Journal of Direct Marketing 7, 1995, pp. 10-19.

20. M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation, Organization Science 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, International Journal of Market Research 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, European Journal of Information Systems 15, 2006, pp. 389-402.
23. T. Dinev, P. Hart, An extended privacy calculus model for e-commerce transactions, Information Systems Research 17, 2006, pp. 61-80.
24. S. Dolnicar, Y. Jordaan, Protecting consumer privacy in the company's best interest, Australasian Marketing Journal 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, Journal of Interactive Marketing 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, Journal of Marketing Research 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, Chemometrics and Intelligent Laboratory Systems 58, 2001, pp. 247-259.
31. J.F. Hair, C.M. Ringle, M. Sarstedt, PLS-SEM: Indeed a silver bullet, Journal of Marketing Theory and Practice 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, Journal of Marketing 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, Journal of Consumer Research 9, 1982, pp. 132-140.
36. J. Hsieh, A. Rai, M. Keil, Understanding digital inequallity: Comparing contnued user behavioral models of the socio-economically advantaged and disadvantaged, MIS Quarterly 32, 2008, pp. 97-126.
37. J. Jacoby, M.S. Matell, Three-point Likert scales are good enough, Journal of Marketing Research 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 Wold, H., Joreskog, K.G. ed. 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, International Information and Library Review 32, 2000, pp. 379-402.
41. Y. Li, Empirical studies on online information privacy concerns: Literature review and an integrative framework, Communications of the Association for Information Systems 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 Quarterly 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, Journal of the Academy of Marketing Sciences 35, 2007, pp. 572-585.
46. R.O. Mason, Four ethical issues of the information age, MIS Quarterly 10, 1986, pp. 5-12.
47. R.C. Mayer, J.H. Davis, F.D. Schoorman, An integrative model of organizational trust, Academy of Management Review 20, 1995, pp. 709-734.
48. D.H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: An integrative typology, Information Systems Research 13, 2002, pp. 334-359.
49. S.J. Milberg, H.J. Smith, S.J. Burke, Information privacy: Corporate management and national regulation, Organization Science 11, 2000, pp. 35-57.
50. G.R. Milne, A.J. Rohm, S. Bahl, Consumers' protection of online privacy and identity, Journal of Consumer Affairs 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, European Journal of Information Systems 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, Decision Support Systems 56, 2013, pp. 103-114.
53. A.N. Mishra, R. Agarwal, Technological frames, organizational capabilities, and IT use: An empirical investigation of electronic producurement, Information Systems Research 21, 2010, pp. 249-270.
54. R. Noonan, H. Wold, Evaluating school systems using partial least squares, Evaluation in Education 7, 1983, pp. 219-364.
55. P.A. Norberg, D.R. Horne, D.A. Horne, The privacy paradox: Personal information disclosure intentions versus behaviors, Journal of Consumer Affairs 41, 2007, pp. 100-126.
56. G.J. Nowak, J. Phelps, Direct marketing and the use of individiual-level consumer information: Determioning how and when 'privacy' matters, Journal of Direct Marketing 9, 1995, pp. 46-60.
57. G.J. Nowak, J. Phelps, Understanding privacy concerns: An assessment of consumers information-related knowledge and beliefs, Journal of Direct Marketing 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, Journal of Advertising 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 erporting behaviors, IEEE Transactions on Engineering Management 56, 2009, pp. 45-60.
60. Y.J. Park, S.W. Campbell, N. Kwak, Affect, cognition, and reward: Predictors of privacy protection online, Computers in Human Behavior 28, 2012, pp. 1019-1027.

61. P. Pavlou, State of the information privacy literature: Where we are now and where should we go?, MIS Quarterly 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, Journal of Applied Psychology 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, European Journal of Information Systems 19, 2010, pp. 181-195.
64. J.L. Rasmussen, Analysis of Likert-scale data: A reinterpretation of gregoire and driver, Psychological Bulletin 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, Academy of Management Review 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, California Management Review 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 Quarterly 35, 2011, pp. 989-1015.
72. H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: Measuring individuals' concerns about organizational practices, MIS Quarterly 20, 1996, pp. 167-196.
73. J. Smith, Privacy policies and practices: Inside the orgnanizational maze, Communications of the ACM 36, 1993, pp. 105-122.
74. M. Sobel, Asymptotic confidence intervals for indirect effects on structural equation models, Sociological Methodology 13, 1982, pp. 290-312.
75. D.W. Straub, Validating instruments in MIS research, MIS Quarterly 13, 1989, pp. 147-169.
76. D.W. Straub, M.-C. Boudreau, D. Gefen, Validation guidelines for IS positivist research, Communications of the Association for Information Systems 13, 2004, pp. 380-427.
77. M. Tenenhaus, V.E. Vinzi, Y.-M. Chatelin, C. Lauro, PLS path modeling, Computational Statistics and Data Analysis 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, Journal of Consumer Affairs 42, 2008, pp. 411-424.
80. H. Van der Heijden, User acceptance of hedonic information systems, MIS Quarterly 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, Journal of Management Information Systems 24, 2008, pp. 73-100.
82. J. Wirtz, M. Lwin, J.D. Williams, Causes and consequences of consumer online privacy concern, International Journal of Service Industry Management 18, 2007, pp. 326-348.

83. H. Wold, Soft modeling: The basic design and some extensions in Joreskog, K.G., Wold, H. eds., Systems under indirect obseration: 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, Journal of the Association of Information Systems 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, Information Systems Research 23, 2012, pp. 1342-1363.
86. S. Youn, Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents, Journal of Consumer Affairs 43, 2009, pp. 389-418.
87. S. Youn, Parental influence and teens' attitude toward online privacy protection Journal of Consumer Affairs 42, 2008, pp. 362-388.

Appendix 1. Tests for non-response 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	-.23304	.12430	-1.875	P < .10
TR	.12425	.10605	1.172	n.s.
TC	.07227	.09128	.792	n.s.
DT	-.22294	.02475	-9.009	P < .01
ID	.10216	.06479	1.577	n.s.
UR	.10292	.07711	1. 335	n.s.
HR	-.08735	.07633	-1.144	n.s.
TP	.03711	.07129	.521	n.s.
GC	.12361	.06808	1.816	P < .10
WI	.02814	.05797	.485	n.s.
RP	.04502	.05264	.855	n.s.
Age	-.267	.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%	.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
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

Perceived Regulatory Protection (PRP)			
For each of the following statements. please state if you tend to agree or not	Scale	Mean	SD
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

Trust in Regulators (TR)			
Overall, how much do you trust the following institutions to handle your personal information safely?	Scale	Mean	SD
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

Trust in Companies (TC)			
Overall, how much do you trust the following entities to handle your personal information safely?	Scale	Mean	SD
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	.949

Data Tracking Concerns (DT)			
How concerned are you about the following risks in relation to your personal data	Scale	Mean	SD
Companies possess information about me that I consider private	1 - 5	1.86	.905
My personal information is used without my knowledge	1 – 5	1.67	.897
My online personal data is used to send me commercial offers	1 – 5	1.64	.897
My behavior and activities can be monitored online	1 – 5	1.92	.983
My identity is reconstructed using personal data from various sources	1 – 5	1.79	.952
My personal data is shared with third parties without my agreement	1 - 5	1.64	.897

Identity Damage Concerns (ID)			
How concerned are you about the following risks in relation to your personal data	Scale	Mean	SD
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	.896
My views and behavior may be misrepresented based on online personal information	1 – 5	2.01	.979
I may be victim of financial fraud online	1 - 5	1.74	.947

Utilitarian Rewards (UR)			
How likely are you to provide personal data for the following reasons?	Scale	Mean	SD
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

Hedonic Rewards (HR)			
How likely are you to provide personal data for the following reasons?	Scale	Mean	SD
To receive valuable information	1 – 5	3.57	1.038
To enjoy, to take pleasure	1 – 5	3.24	1.096
To make a good action, to help	1 – 5	3.30	1.086
To connect with others	1 – 5	3.50	1.111

Technical Protection (TP)			
I usually protect my personal data and identity in the following ways	Scale	Mean	SD
Scan data with anti-spy ware	1 – 4	3.09	.997
Update virus protection	1 – 4	3.26	.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	.977
Check that the transaction is protected or the site has a safety badge before I enter valuable personal data	1 – 4	3.05	.986

General Caution (GC)			
Adapt my personal data so that no linking between profiles is possible	1 – 4	2.24	1.019
Read the privacy policy of web sites	1 – 4	2.26	.915
Change the security settings of my browser to increase privacy (removed)	1 - 4	2.43	1.002

Withholding (WI)			
Give a minimum of information	1 - 4	2.76	.823
Do not give personal details	1 - 4	2.38	.781

Regulatory Preferences (RP)			
What do you think are the efficient ways to protect your identity and privacy	Scale	Mean	SD
Give users more direct control on their own identity data	1 - 4	2.92	.756
Allocate more resources to monitoring and enforcing existing regulations	1 - 4	2.98	.757
Require that service providers take greater care of their customer's identity	1 - 4	3.21	.803
Provide formal education on safe identity management	1 – 4	3.00	.788
Set up clear guidelines for safe identity management, online and offline	1 - 4	3.14	.758

Internet activities (used in post-hoc analysis)	
Do you do the following activities on the Internet? (Tick all that apply.)	Percentage ticked
Check email (B)[10]	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 website (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	54%
Keep a web-log (or what is called a blog) (A)	8%
Use peer-to-peer software to exchange movies, music, etc. (A)	17%

[10] (B) denotes a "basic" task; (A) denotes an "advanced" task.

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
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
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