Cultural and generational influences on privacy concerns: a qualitative study in seven european countries

Caroline Lancelot Miltgen, Dominique Peyrat-Guillard

CULTURAL AND GENERATIONAL INFLUENCES ON PRIVACY CONCERNS: A QUALITATIVE STUDY IN SEVEN EUROPEAN COUNTRIES

Accepted for publication in the

European Journal of Information Systems

Caroline Lancelot Miltgen (First and Corresponding Author)

Angers University
GRANEM Research Center

UFR de Droit, d'Economie et de Gestion
13, Allée François Mitterrand
BP 13633
49036 Angers Cedex 01
FRANCE

Tel: 00 33 665 012 704
Fax: 00 33 241 962 196
Email: caroline.miltgen@univ-angers.fr

Dominique Peyrat-Guillard

Angers University
GRANEM Research Center

Caroline Lancelot Miltgen (Ph.D., University of Paris Dauphine) is Associate Professor of Marketing at Angers University, France. Her research concentrates on information privacy and technology adoption. She has presented papers at international conferences and has published her work in French and international scholarly journals.

Dominique Peyrat-Guillard (Ph.D., University of Poitiers) is Associate Professor of Human Resource Management at Angers University, France. Her research deals with Organizational Behavior and statistical analysis of textual data. She has presented papers at international conferences and has published her work in French and international scholarly journals.

CULTURAL AND GENERATIONAL INFLUENCES ON PRIVACY CONCERNS: A QUALITATIVE STUDY IN SEVEN EUROPEAN COUNTRIES

Abstract

This research examines how European citizens decide to disclose and protect their personal data and thereby reveals cultural and generational divides. Focus group discussions featured either young people, aged 15 to 24 years, or adults, between 25 and 70 years of age, and were conducted in seven EU member states. The results of a computer-aided text analysis with two complementary software packages suggest similarities and differences in participants' views and privacy concerns. Responsibility is relevant to personal data management, which represents a hotly contested issue. A geographical north–south divide appears for the importance of responsibility as opposed to trust. Moreover, people regard disclosure differently in the south (as a choice) and east (as forced) of Europe. Younger people express more positive attitudes toward data management, feel more responsible, and are more confident in their ability to prevent possible data misuse. Their lower privacy concerns and greater protective behaviours (i.e., a potential reversed privacy paradox) may help explain contradictory results in prior literature. These results offer significant and useful theoretical, managerial, and policy implications.

Keywords

Privacy concerns, Personal data disclosure, Focus groups, Computer-aided text analysis, Cultural variation, Generation divide

Funding

This study was funded by the European Commission IPTS (Institute for Prospective Technological Studies) Joint Research Centre (EC JRC IPTS Contract No. 151592-2009 A08-FR).

Acknowledgements

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

Introduction

With advances in information technology (IT), individual data can be collected, aggregated, and analysed more quickly and in greater volume than ever before (Malhotra et al., 2004). These practices raise increasing concerns about information privacy—defined as the ability to control information about oneself (Smith et al., 1996a). Although this concept existed long before IT changed its occurrences, impacts, and management (Belanger & Crossler, 2011), Mason's (1986) prediction that information-related privacy would become an increasingly critical concern has proved true. Surveys show that 85 percent of US adults believe it is very important to control access to their private data (Madden et al. 2007), and 72 percent express concerns about whether firms track their online behaviour (Consumers Union 2008). With the worldwide development of digital technologies, privacy continues to be critically important to industries, governments, and the global community (Davison et al. 2003). Wang and Emurian (2005) even show that information privacy concerns are the most formidable barrier to people engaging in e-commerce.

To date, research on information privacy mainly seeks to explain differences in the levels of privacy concerns or explore their effects on dependent variables, such as willingness to provide personal information or transact online (Belanger & Crossler, 2011). However, conflicting findings have hampered a clear understanding of people's views on privacy and impeded the full adoption of digital innovations and related e-services, as well as the development of a fully protective policy framework. The first aim of this paper is thus to answer a simple research question: On which issues do people really focus when their privacy may be at risk? That is, which criteria do people take into account when deciding whether to disclose or guard their personal data during digital transactions with public or private entities? Determining these criteria can support the design of useful, protective electronic tools and systems, as well as policy measures that can address privacy concerns.

Although information privacy in general and data use and control issues in particular are universal matters, we concur with scholars who argue that the precise concerns and responses to data requests depend on users' characteristics, including their culture (e.g., Dinev et al., 2006; Posey et al., 2010) and age (e.g., Moscardelli & Divine, 2007). Although some contributions note these influences, we lack an understanding of the differences that these characteristics provoke in relation to privacy concerns. The conflicting results regarding the effects of individual antecedents have prompted calls for cumulative research. Because we do not know exactly how individual antecedents affect privacy concerns, we cannot determine which solutions effectively protect individual privacy (Li, 2011).

Most literature on the impact of privacy takes place in a single country, namely, the United States (Belanger & Crossler, 2011). The few studies that have adopted a cross-country perspective mostly assess the differences between the United States and another country. Instead, we require 'a richer focus on international dimensions of privacy research' (Smith et al., 2011, p. 1007), along with 'deeper insight into privacy issues from countries other than the US' (Li, 2011, p. 471), and 'more studies on information privacy in multiple countries using preferably nonstudent populations' (Pavlou,

2011, p. 979). Despite some general agreement about the impact of culture on privacy, contradictory results call for more research too. To fill this gap, we focus on the privacy concerns of citizens from seven European countries and attempt to answer a second research question: How does culture influence privacy concerns and related behaviours, in particular for people from geographically proximate nations in Europe?

In addition to culture, age dictates how people relate to IT, a phenomenon that influences their privacy concerns (e.g., Moscardelli & Divine, 2007). Young people who have grown up with the Internet tend to use social media more than older people, though this usage does not mean they are unconcerned about online privacy. Lenhart and Madden (2007) find that teenagers use various techniques to obscure their real location or personal details on social networking sites (SNS). New studies thus need to reframe the issue to determine the main privacy concerns of young people compared with those of older adults. We therefore investigate a third research question: How do people of different ages vary in their attitudes toward privacy and their subsequent behaviours?

To answer these three questions, this study undertakes a qualitative assessment of Europeans' attitudes toward privacy, personal data disclosure, and protection using 14 focus groups across seven EU27 countries. Our work departs from most literature on privacy and its positivist paradigm, which provide controversial insights into how privacy concerns affect user behaviour (Krasnova et al., 2009). Research might suggest that people are reluctant to disclose personal information (Kelly & McKillop, 1996), yet in practice, many people voluntarily do so, particularly on blogs and online platforms. Existing quantitative research cannot explain these contradictions, nor reveal how people worried about privacy make self-disclosure decisions. To provide new insights, we adopt a qualitative perspective, with which we identify the threats that are of the greatest concern to users and determine how they affect the behavioural outcomes. Our research across seven countries also extends beyond studies that rely solely on student populations and answers the call for more diverse research populations (e.g., Belanger & Crossler 2011; Smith et al., 2011).

By cross-referencing privacy attitudes and concerns with demographic details, this work helps refine existing models. In particular, we outline the potential consequences of cultural and generational differences to help explain the unresolved conflicts between stated motivations and observed behaviours. We also offer advice to policy makers about how to adapt their regulatory framework to match EU citizens' opinions and behaviours. Finally, from a methodological point of view, we demonstrate the potential of rigorously applied qualitative techniques to produce useful data and complement quantitative research.

Research foundations

Although 'General privacy as a philosophical, psychological, sociological and legal concept has been researched for more than 100 years in almost all spheres of the social sciences' (Smith et al., 2011, p. 992), we lack any real consensus about what it means (Solove, 2006), in part because every discipline has a different conceptualisation. Smith et al. (2011) note that the definition of privacy can

be classified broadly as either value- or cognate-based. The former views privacy as a human right integral to society's moral value system, popularised by Warren and Brandeis (1890) as 'the right to be let alone'. The latter was introduced by psychologists and cognitive scientists who considered privacy in relation to the individual mind, perceptions, and cognition. In this case, privacy is about control of physical space and information; Westin (1967, p. 7) defines this form as a 'voluntary and temporary withdrawal of a person from the general society'.

Information privacy

Although Clarke (1999) identifies four dimensions of privacy—privacy of a person, behaviour privacy, communication privacy, and personal data privacy—extant literature mainly focuses on the two last subsets. Much modern communication is digital and stored as information, so they reasonably can be merged into a single construct, information privacy. Although information privacy also can be defined in multiple ways, we concur with most scholarship, which refers to an individual desire to control or have influence over the acquisition and potential secondary uses of personal data (e.g., Belanger et al., 2002; Belanger & Crossler, 2011). In addition, 'because of the near impossibility of measuring privacy itself and also because the salient relationships depend more on cognitions and perceptions than on rational assessments' (Smith et al., 2011, p. 997), we use a proxy common in privacy research, namely, privacy concerns. Information privacy concerns reflect an anticipation of future potential losses of privacy (Culnan & Armstrong, 1999; Milberg et al., 2000), defined more broadly as an 'individual's subjective views of fairness within the context of information privacy' (Malhotra et al., 2004, p. 337). For this study, we focus on individual perceptions of what happens to information provided to public or private parties in a digital form, such as via the Internet. Following Smith et al. (2011), we use 'privacy' to refer to information privacy, particularly online or digital.

Situationality

Smith et al. (2011) note several factors that can change the meaning of information privacy. Across the vast range of relevant contexts and situations, privacy cannot be served by a single, simple definition (Johnson 1992); it means different things to different people, with contextual roots and consequences (Bennett 1992). Context, or the 'stimuli and phenomena that exist in the environment external to the individual' (Mowday & Sutton, 1993, p. 198), is usually specific to the time, location, occupation, culture and rationale (Bansal et al., 2008) that surrounds a particular concept and/or decision. It thus moderates (Milberg et al., 1995; Smith et al., 1996a; Bellman et al., 2004; Dinev et al., 2006) or directly influences (Malhotra et al., 2004) the nature of privacy relationships.

Antecedents and consequences

The APCO model (Smith et al 2011) provides a useful way to summarize the previous scholarly work about privacy, particularly in the IS literature. This model considers privacy concerns (PC) as the central construct to study, which has both Antecedents and Outcomes. The antecedents of PC in previous literature represent three groups of factors (see Figure 1): (1) individual, (2) contextual, and

(3) macro-environmental. In prior investigations, the mixed results regarding the influence of any of these factors spark calls for deeper considerations; in this study, we focus on the influence of age and culture. Individual-level factors thus far have been the most frequently analysed antecedents of PC, and some categorisations already exist (e.g., Li, 2011). We identify six kinds of individual factors that may influence PC (see Figure 1). Most of them pertain to fundamental, individual traits, such that prior literature considers their impacts on PC separately from their contexts (Li, 2011). Age is particularly interesting as it has a clear influence on information processing and affects interaction with technology (Morris et al., 2005). The two macro-environmental factors most often tested with regard to their impacts on PC are cultural values and regulatory structures. Culture exhibits a complex relationship with PC (Milberg et al., 2000; Bellman et al., 2004) and is therefore of particular interest.

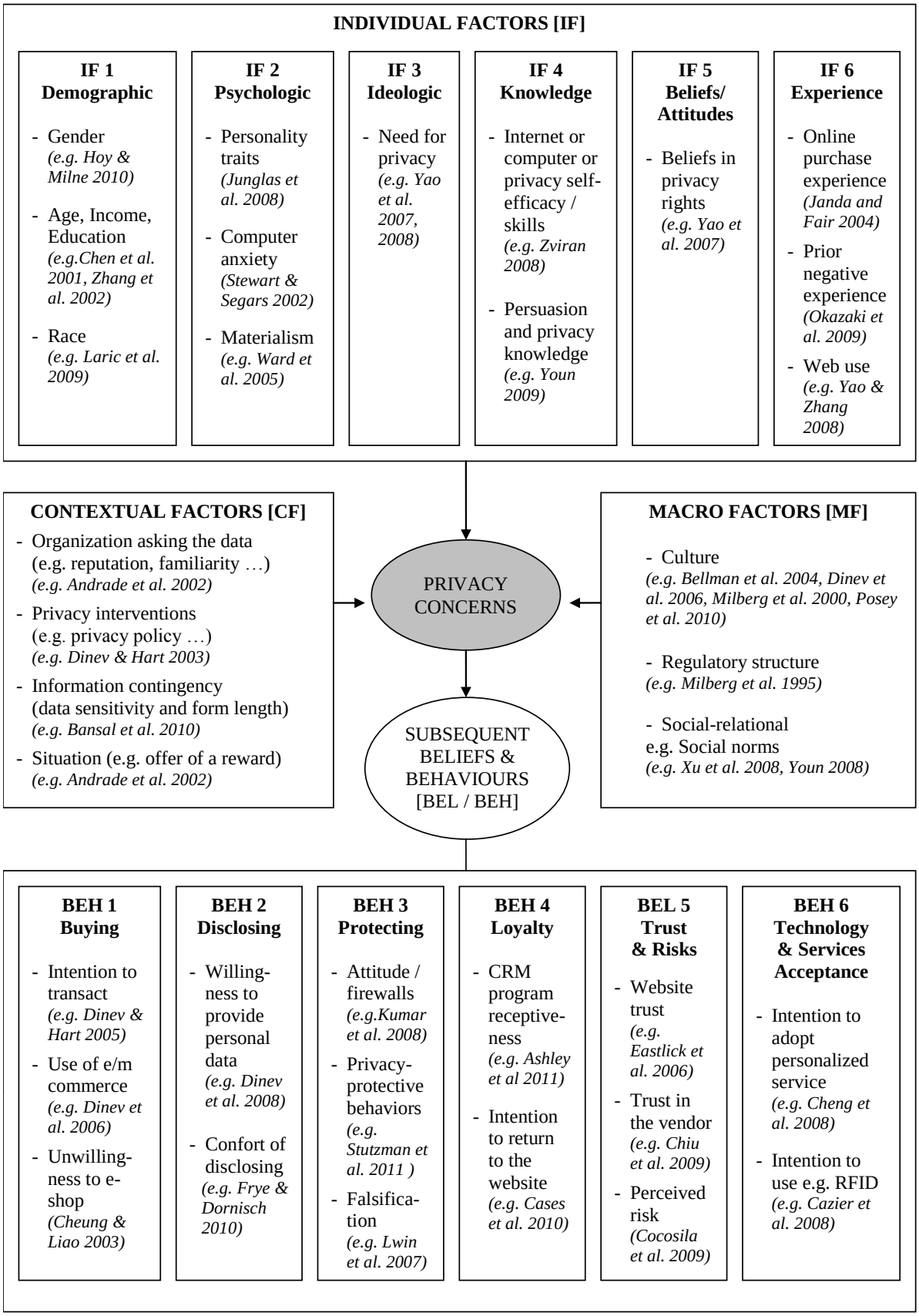
The consequences of PC also have received substantial attention, mostly in analyses of behavioural intentions (e.g., willingness to provide or protect information). Some outcomes cannot be classified effectively in this frame though, so Li (2011) suggests more detailed categorisations. Again, we identify six main outcomes of privacy concerns: buying, disclosing, protecting, loyalty behaviours, trust and risk beliefs, and technology or service acceptance. On the basis of the APCO model (Smith et al. 2011), Figure 1 reveals the direct impact of PC on subsequent outcomes, though this influence may be mediated by perceived privacy risks and trust (e.g., Van Slyke et al., 2006.). Trust, information privacy, and disclosure are closely linked concepts, usually examined simultaneously, though their exact relationship remains a topic of debate.

The importance of trust

Debates related to privacy and digital technologies often integrate trust, in its various forms and versions: unconscious, unwanted, forced, or unrecognised (Baier, 1986). Rousseau et al. (1998, p. 395) define trust as 'a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another'. Uncertainty, vulnerability, and the possibility of avoiding risk or making a choice based on judgement are necessary conditions (Blomqvist, 1997), as is the presence of information. Trust is mainly considered a good thing, but its dark side can create unwanted obligations and lock-in effects (Dietz et al., 2011). A need for trust creates a potential power asymmetry, somewhat underplayed in previous studies (Dietz et al., 2011).

Trust also plays a key role in online interactions and relationships (Fukuyama, 1996), where people have more difficulty assessing others' potential for harm or goodwill (Friedman et al. 2000). Trust relates to both information privacy and disclosure (Fogel & Nehmad, 2009), and perhaps mediates between them (e.g., Dinev & Hart, 2006); is an antecedent (e.g., Bélanger et al., 2002; Eastlick et al., 2006) or a consequence (Malhotra et al., 2004; Bansal et al., 2010). Trust could also moderate the relationship (Bansal et al., 2008) so that PC have a weaker effect on behaviour, relative to trust (e.g. Ba & Pavlou, 2002). The substantial controversy in this area calls for more research to offer a deeper understanding of the relationship among privacy, trust, and behaviours.

Figure 1. Antecedents and outcomes of PC (adapted from Smith et al. 2011 and Li 2011)



In reference to the APCO model (Smith et al. 2011), IF, CF and MF are antecedents; BEL and BEH are outcomes. For the references cited, along with some additional insightful references, see Li (2011).

Hypothesis development

This research aims to determine which privacy-related issues people really focus on and identify their behavioural consequences. We investigate the impact of culture and age, in consideration of the controversial results in previous literature. By considering people's perceptions of key privacy-related issues, we offer additional insights and bring to light a new, in-depth understanding of the factors that can affect data disclosure.

Impact of culture on privacy

Prior literature has emphasised the relationship between people's culture and their valuation and interpretation of privacy (e.g., Milberg et al., 2000). Culture shapes values and expectations (Cullen & Reilly, 2007) and largely determines how people perceive disclosure issues (e.g., Milberg et al., 1995). Palfrey and Gasser (2008, p. 53) confirm 'many regional differences in how online privacy is treated in cultures around the world'. Even citizens of countries in similar geographical areas (e.g., Europe) might display significant variation in their privacy concerns and online activity (e.g., Bellman et al., 2004). Fukuyama's (1996) work on conceptions of trust distinguishes not only distant cultures, such as Japan and the United States, but also European neighbours, such as France and Germany. Because culture largely determines privacy concerns (e.g., Bellman et al., 2004; Dinev et al., 2006), any investigations of this topic should account for cultural differences, a requirement that seems increasingly relevant when we consider that such enquiries are rare among European national cultures.

Conducting cultural research is challenging, considering the myriad definitions of culture available (Straub et al., 2002). Sackmann (1992) notes that culture has been framed as ideologies, sets of beliefs, basic assumptions, shared sets of core values, important understandings, and the collective will. Culture can also include explicit artefacts, such as norms and practices (Delong & Fahey, 2000), symbols (Burchell et al., 1980), language, ideology, rituals, and myths (Pettigrew, 1979). To date though, the most popular conceptualisation of national culture is Hofstede's (1980) taxonomy of five cultural dimensions: power distance, individualism, masculinity, uncertainty avoidance, and long-term orientation. Various taxonomies of culture (e.g., Trompenaars, 1996) tend to concur that certain sets of values persist in all countries but vary in their magnitude. Hofstede's (1980) approach admittedly suffers some limitations, but it is coherent with prior information systems research, in which more than 60 percent of cross-cultural studies use at least one Hofstedian dimension (Leidner & Kayworth 2006). Furthermore, cross-cultural research largely confirms that the relationship between people's national culture and valuation of privacy reflects Hofstede's (1991) framework (e.g., Milberg et al., 2000; Bellman et al., 2004; Dinev et al., 2006; Posey et al., 2010). Thus, we adopt Hofstede's (1991, p. 5) definition of national culture: 'collective programming of the mind which distinguishes the members of one group or category of people from another'.

The key cultural dimensions related to privacy include power distance, or the degree to which a society tolerates greater or lesser levels of inequality, and individualism (IDV) versus collectivism (COL), defined by the existence of strong cohesive groups and extended families that protect the

individual in exchange for loyalty (Cullen, 2009). Individualism is pivotal (Allik & Realo, 2004) to cultural systems (Oyserman et al., 2002) and appears in a range of disciplines, including philosophy, history, anthropology, sociology, psychology, and business (Triandis, 1995). Kagitcibasi (1997, p. 3) notes that 'about one-third of recently published studies cited [individualism/collectivism] as at least a partial explanation of observed cross-cultural differences'. It also is the most studied cultural dimension in information systems literature (Shin et al., 2007; Posey et al., 2010).

Some such research indicates that people from highly individualistic national cultures have fewer privacy concerns and are more comfortable with high levels of data disclosure (Ting-Toomey, 1991). For example, Maynard and Taylor (1996) find that Japanese students (IDV = 46) are more concerned about privacy than US students (IDV = 91). An IBM (1999) privacy survey also indicates that Americans are half as concerned as Germans (IDV = 67). In contrast, other studies indicate a positive association between individualism and privacy concerns (Milberg et al., 2000; Posey et al., 2010). Bellman et al. (2004, p. 315) agree that collectivistic cultures 'have a greater acceptance that groups, including organizations, can intrude on the private life of the individual'. These contradictory results suggest an ongoing discussion about whether individualistic national cultures are more or less concerned about privacy. We seek to clarify this complex relationship by predicting:

> *H1: People from different countries in Europe differ in their privacy concerns and declared behaviours. In particular, people from collectivist countries tend to exhibit more trust and less reluctance to disclose information than those from individualist countries.*

Age and privacy

Regardless of their national culture, people's conceptualisations of privacy and disclosure are dynamic over time (e.g., Boyd, 2007; Livingstone, 2008). We pursue a better empirical understanding of young people's online practices, in comparison with an older population's consideration of privacy, to determine how these beliefs influence online behaviours by both populations. Some prior literature indicates that children and teenagers show less concern than adults about privacy (e.g., Moscardelli & Liston-Heyes, 2004; Palfrey & Gasser 2008). For example, three-quarters of young people (college students) are concerned with the privacy and security of passwords and Social Security and credit card numbers, but they are not afraid of sharing personal data on social networking sites that they somehow regard as private spaces (Jones et al., 2009). Teenagers consider SNS a place where they can socialise, away from the watchful eyes of parents and teachers (Marwick et al., 2010). They express less worry about data protection than about what their teachers would learn if granted access to their profile. Young people consider themselves reasonably Internet-literate and technologically aware, which should enable them to deal with privacy risks (Life Support, 2010). Although they know that others misrepresent themselves on occasion, their strong (sometimes misplaced) feelings of being in control can expose them to unwanted dangers (Life Support, 2010). Awareness of SNS privacy settings usually does not affect their information provision (Govani and Pashley, 2007), though young people

sometimes 'believe incorrectly that the law protects their privacy online and offline more than it actually does' (Hoofnagle et al., 2010, p. 4). Other factors (e.g., value of disclosure, trust, self-efficacy) have stronger effects in reducing youngsters' privacy concerns (e.g., Youn, 2005, 2009; Moscardelli & Divine, 2007; Hoofnagle et al., 2010; Marwick et al., 2010).

Yet few empirical studies can confirm that young people actually express fewer privacy concerns than adults. Recent literature (Table 1) indicates young people are more, less, or equivalently preoccupied with privacy. Studies focusing on the consequences of young people's privacy concerns similarly offer contradictory results, including both increased protective behaviours and the development of risky behaviours (Table 2).

Overall though, young people differ from adults when it comes to privacy issues. According to Livingstone (2008), the question of what people show to others and what they keep private tends to prompt the liveliest interviews with young people, suggesting their intense interest in privacy. This author suggests that children seek privacy as a means to an end, not as an end in itself. In addition, young people participate in online interactions designed especially to increase the amount of personal data they reveal, such as in SNS. Therefore, though young people may aspire to increased privacy, we predict that their concerns remain lower than those of adults and hypothesise:

H2: People from different age groups differ in their privacy concerns and declared behaviours. Young people have more positive views of privacy-related issues than older people.

Research method

We aim to investigate the privacy concerns of varied European people using their own perceptions and words and to explore the link of these views with their subsequent behaviours. We also investigate some of the contradictions and paradoxes in previous literature. Therefore, we have chosen a qualitative approach, using focus groups, to determine if any pattern emerges from discussions and interactions among the participants.

Rationale for the use of focus groups

This study uses focus groups, which are especially valid for demonstrating values and cognitions that are common or uniform in a particular social group (e.g., young people). No other methodology is as straightforward for uncovering broader social values possessed by specific segments of consumers in relation to a specific issue (Mendes De Almeida, 1980). The method is notably useful for exploring people's knowledge and experiences and can reveal not only what people think but also how they reason and why (Kitzinger, 1995). Focus groups 'capitalize on the interaction within a group to elicit rich experiential data' (Asbury, 1995, p. 414). Kitzinger (1995, p. 299) notes: 'The idea behind the focus group method is that group processes can help people to explore and clarify their views in ways that would be less easily accessible in a one-to-one interview'. Focus groups are also particularly sensitive to cultural variables, which is why they are so common in cross-cultural research.

Table 1. Privacy concerns among young people and adults

Young people less concerned than adults		**Young people more concerned than adults**		**No difference**	
Results	*References*	*Results*	*References*	*Results*	*References*
Children and teenagers show less concern about privacy than adults	Moscardelli & Liston-Heyes, 2004; Palfrey & Gasser 2008	Young users are more likely to adopt a private profile than older users, perhaps due to increased tech-savviness in younger groups	Caverlee & Webb, 2008	Privacy attitudes among US young adults (18–24 years) do not differ from those of older adults. In reading privacy policies, there are no statistical differences.	Hoofnagle et al., 2010
Less concern about sharing information on SNS	Jones et al., 2009	Teens are more vigilant than adults in privacy-protecting behaviours	Moscardelli & Divine, 2007; Lenhart et al., 2007; Caverlee & Webb, 2008		
		The likelihood of providing personal information increases with age	Lenhart & Madden, 2007; Steeves & Webster, 2008		

Table 2. Consequences of young people's privacy concerns on subsequent behaviours

Protective behaviours		**Risky behaviours**	
Results	*References*	*Results*	*References*
Younger teens are most likely than adults to post fake information.	Lenhart & Madden, 2007; Moscardelli & Divine, 2007; Lenhart et al., 2007; Caverlee & Webb, 2008	Privacy-concerned young adolescents are not accustomed to fabricating personal information or do not recognise the importance of remaining anonymous.	Youn, 2009
Most teens restrict access to their online profiles. Although changing privacy settings is difficult and confusing, it is becoming more common	Marwick et al., 2010; Lenhart & Madden, 2007; Livingstone, 2008, Gross & Acquisti, 2005; Lampe et al., 2008	Teens may not be vigilant in protecting themselves from privacy risks.	Turow & Nir, 2000
An adolescent sample shows higher means on all four privacy-protecting behaviours and lower means on two privacy-divulging behaviours. Teens may be more vigilant than adults.	Moscardelli & Divine, 2007	Heavy Internet usage combined with underdeveloped socialisation skills make adolescents vulnerable to privacy risks.	Moscardelli & Divine, 2007
Teens engage in privacy-protecting behaviours if they are concerned with privacy, perceive information risk, or see themselves as vulnerable. They also seek more information by reading privacy statements.	Youn, 2009	Most youth do not read privacy policies; when they do, they rarely act on that information.	Youn, 2005

Organization of the focus groups

We organized 14 focus groups in seven European countries, each of which included eight to twelve participants (Cox et al., 1976; Fern, 1982). The average duration of each focus group was 90 minutes, and it was moderated in each country by scholars from partner universities, chosen for their experience and facility in discussing the topic. The recruiting method relied on demographic controls as a basis for selecting respondents (Prince, 1978). This information came from a very short questionnaire that all participants completed before the focus groups, containing questions about their demographic and socioeconomic status. The survey data defined the recruiting process and enabled us to link every comment with the speaker's demographic profile, including nationality and age.

Moderators received detailed information that described their responsibilities to make the environment a safe place for group participants, help them feel at ease, create a non-judgmental stance, moderate the input of more dominant group members, and motivate quiet participants to talk. To help structure the discussion and ensure consistency in the issues covered across the countries, all moderators were furnished with an interview guide (available on request) that detailed the major inquiry lines (Merton & Kendall, 1946) and provided discussion prompts. To avoid what Merton et al. (1990) call the fallacy of adhering to fixed questions, the research design allowed minor variations and thus accommodated the unique aspects of each group. All the discussions were run in the native language of the participants, which was also the native language of the moderators, so they could facilitate discussions of delicate topics, such as privacy. Because the discussions were run by different moderators in various languages, we trained and briefed them to ensure the groups were run similarly.

Sampling method

We carefully chose the countries for the focus groups, to ensure sufficient cultural differences and similarities. We focused on a target population that reflected the diversity of practices and views across Europe. We divided Europe in four geographical blocks:

1. Denmark, Finland, Sweden, Estonia, Latvia, Lithuania (Northern Europe)
2. Bulgaria, Czech Republic, Hungary, Poland, Romania, Slovakia, Slovenia (Eastern Europe)
3. Austria, Belgium, France, Germany, Ireland, Luxembourg, the Netherlands, United Kingdom (Western Europe)
4. Cyprus, Italy, Greece, Portugal, Spain, Malta (Southern Europe)

For each block, we sought two countries in which to run the focus groups, to ensure diversity within the same block and across all blocks, according to the criteria in Appendix 1. Estonia (Block 1) was an interesting country given its high e-government availability and low access and usage levels. Poland and Romania (from Block 2) offered an interesting comparison with Estonia, because they exhibit very different levels of IT development. France and Germany (Block 3) were retained as leading countries in Europe. Spain (from Block 4) is similar to France in its IT development but differs in its cultural and geographical background and progress. Greece (Block 4) offers an interesting

comparison with Spain, with much lower IT development. These countries also vary in their Internet usage rates, from low (Romania 30%, Greece 31%) to moderate (France 62%, Estonia 58%, Spain 51%, Poland 48%) to high (Germany 75%). These seven countries effectively represent the European dispersion of Internet use; their average is 54.6 percent, very close to the European average of 57.2 percent. Finally, the countries have relatively equal geographical representation throughout Europe, with two countries in each of the four blocks except for Block 1.

We attempted as much as possible to ensure diversity in the focus groups in terms of demographics (see Appendix 2). Along generational lines, we ran two focus group in each country, one with young people (15–24 years of age) and another with adults (25–70 years of age). Caverlee and Webb (2008) consider people from 18 to 24 as young adults. We decided to interview people younger than 18 years but older than 15 years, to include teens but not children, who may have difficulties expressing their ideas. For adults, we did not interview people older than 70, again to ensure participants would be able to express their ideas and feel at ease. In the data analysis, all participants were identified by their answers to the questionnaire, so we could further divide the age range into more specific categories: 15–18, 19–24, 25–44, 45–60, and +61 years. The two first categories divide young people (under 18) who are still in high school from those (19–24) who are at university or work. The next two categories represent young adulthood (25–44) and middle age (45–60), and then older people enter the + 61 category.

Results

Focus groups offer a special opportunity for applying computer technologies for data analysis (Javidi et al., 1991). We thus applied computer-aided text analysis (CATA) 'to systematically, comprehensively, and exhaustively analyze' (Gephart, 2004, p. 259) the data. This extremely rich, well-established approach provides good effectiveness (Lebart & Salem, 1994).

We ran two CATA using dedicated software packages (Lebart & Salem, 1994), which support a systematic analysis of the corpus (Gephart, 2004) and suggest a more objective measure of the differences in attitudes according to specific variables, compared with the one we would have obtained with a manual content analysis. The software packages can identify patterns and interconnections, which are then subjected to the researchers' interpretations. Between the epistemological positions of constructivism and positivism, we chose an abductive approach that combines empirical facts with heuristic frames of reference (Staat, 1993). This approach goes back and forth between the empirical results and the theories and concepts used to understand the empirical data. The objective is to construct intelligible representations, through a progressive construction of knowledge in relation to extant literature. It relies on exploration and the capacity to reveal the unexpected, which means integrating observation and reasoning in an approach that combines three inferences—abduction, deduction, and induction—in a loop that models scientific reasoning (Peirce, 1931-1935).

We used two software packages: Alceste to analyse discourse and content through descending hierarchical classifications (DHC) and WordMapper to run factorial analyses of correspondence (see Appendix 3). Alceste reflects the influence of both multidimensional statistical analysis (Benzécri, 1981) and Peirce's (1931–1935) propositions on semiosis for the treatment of text and interpretation of analysis results. It can quantify texts to extract significant structures and draw out the essential information from textual data. Research has shown that these structures are closely linked to the distribution of words in a text, which is rarely random (e.g., Benzecri, 1981; Reinert, 1986). Alceste thus can describe a text according to its formal structure, in terms of the co-occurrence of words in statements in a given corpus. We obtain a classification of answers that reflects similarities and dissimilarities in vocabularies, using DHC to conduct successive splits of the text. The DHC classes separate words, not individuals, such that they reflect the main topics raised during the overall discourse of all participants. Alceste performs two classifications to limit the influence of the automatic segmentation of the corpus and to ensure stability. To reinforce and complement this approach, we used WordMapper software, which runs a correspondence factor analysis (CFA) to detect possible associations and oppositions among variables (e.g., nationality, age) and words. The projection of these variables and words onto a set of factorial axes produces two-dimensional graphs, which support our interpretation of the results.

Validity and reliability

Qualitative research assumes that reality is constructed, multidimensional, and ever-changing; the methods to ensure the results are valid and reliable thus differ from those used in the positivist paradigm. The people and settings examined are rarely randomly selected, so qualitative studies offer weak population validity for generalising from the sample to a broader population. Qualitative researchers focus on documenting particularistic, rather than universalistic, findings. That is, we are not seeking to establish laws but rather to understand the world from the perspectives of those in it.

Different strategies can strengthen the validity and reliability of a qualitative study (Guba & Lincoln, 1981; Merriam, 1988; Patton, 1991). We used low inference descriptors (participants' sentences); reflexivity (through CATA); thick study descriptions; theoretical generalisation (through sample diversity); standardisation (same protocol for each country); a triangulation of data, methods, investigators, and theory; and peer-review examinations to affirm the quality of the results. These tactics help guarantee, as much as possible, that the results are plausible, credible, trustworthy, and defensible, and therefore considered valid and reliable.

Our first analysis using Alceste software included all 139 participants' discourses. The corpus of 113,754 total words included 5939 separate forms (i.e., different words). After lemmatisation, which reduced the words to their roots, we retained 1202 words. In this first stage, Alceste divided the corpus into 2651 contextual units (CU; equivalent to a sentence), though only 1590 CUs were used for the classification. The percentage of CUs classified in the whole corpus was 60 percent, a good result for

qualitative discussions (Reinert 1998). The Alceste program then established a data matrix to check for the presence or absence of each word in each CU. Only words that appeared more than four times were retained. The iterative process of defining classes of words associated in the same context, using the DHC algorithm (Benzecri, 1981), aimed to maximise the chi-square criterion (Reinert, 1990). Alceste software can identify the most representative parts of participants' discourses for each topic (chi-square > 10.8, significant at the 0.1 percent level, Appendix 4).

Global privacy concerns and declared behaviours of European citizens

The Alceste results show five main issues in the opinions expressed by the focus group participants. The first deals with opinions pertaining to personal data management; the last four reflect the main foci of privacy concerns: control, protection and regulation, trust and responsibility.

Personal data management. This first issue mainly refers to personal data disclosure. As Table 3 reveals, most participants find the collection of personal data intrusive; some lie to obtain a sense of pseudo-anonymity. Others consider data disclosure a quasi-compulsory act, required to obtain the desired e-services. Some participants recognise that data disclosure may offer benefits, so they believe users should not regard it necessarily as a constraint or imagine undesirable consequences. Still other respondents cite a trade-off between constraints/risks and benefits. Yet most respondents advise disclosing only privacy-insensitive data and only to people and organizations they know well or trust.

Table 3. Personal data management

Opinions about personal data management		**Gender**	**Country**	**Age Range**	**Chi-square**
Pseudo-anonymity	'But the only thing necessary for that is our email. What do they need our name and surname for? So, why not give fictitious ones and a real email?'	F	Poland	19–24	23
Compulsion	'One hasn't really got a choice. For example when pursuing some goal such as getting a new email address or a new account. One is basically forced to do it. Well not all information, but the most important data. And you have to disclose it. Yes, they do charge a minimal fee.'	M	Germany	15–18	13
Benefit	'You disclose your data because no more than a name and an address is required, that is used by companies to send you promotion leaflets and information staff, which are often for your benefit'.	M	Greece	19–24	15
Constraints	'I easily give my name, first name and my address. When we must use Internet I do not ask myself all these questions. It's paranoia to think that it will be stolen.'	F	France	25–44	15
Trade-off	'It must be that one decides according to the circumstances, since if one doesn't disclose any data, then I can just as well stop using the Internet. It already starts for	M	Germany	+61	24

	me to obtain an email address, I have to divulge it. It will be somewhere in between. Not revealing anything won't work.'				
Sensitivity	'It depends on the data you disclose; it depends on how close to me they are and on how private and secure this data is.'	F	Greece	19–24	14

Privacy and control. The second issue, as detailed in Table 4, relates to the control foci and indicates that people are aware of the possibility of 'function creep', which leaves them anxious about how to ensure information elicited for one purpose is not used for other purposes. For most respondents, personal data disclosure represents a loss of control and even a breach of privacy. Many participants are afraid of such intrusions, because they consider the risks of data misuse very high and a future (i.e., not immediate) threat therefore difficult to anticipate.

Table 4. Privacy and control

Opinions about privacy and control		**Gender**	**Country**	**Age Range**	**Chi-square**
Function creep	'How can I be sure that this data will only be used for this purpose and no other?'	F	Greece	19-24	19
Loss of control	'As soon as you put information on the Internet you lose control of what you have and you no longer control anything in fact.'	F	France	19-24	23
Privacy breach	'But I believe that we're going more and more toward the breach of privacy of people, and we're going more and more toward dictatorship.'	F	France	45-60	18
Misuse	'I mean, these risks are difficult to anticipate. Because, the risk lies in improper use of this data. A bank won't use it against us, but this data may leak out from the bank's database. Someone may take that data away, and we can't anticipate what use this person will make of it.'	M	Poland	+ 61	11
Future risks	'But I think that Facebook will hurt the actual generation for work later. They really displayed and this will be prejudicial. Secondary school pupils don't realise that there can be a potential danger.'	M	France	45-60	15

Protection and regulation. This issue refers to protection behaviours declared by participants. They clearly express a need for more efficient and secure regulations and resent power imbalances. They do not know how to ensure that their rights will be respected (redress) and often use self-protective measures, such as not registering online, as described in Table 5.

Trust. As we see in Table 6, two major trust-related themes emerge as main concerns. First, the participants trust organizations when they perceive no risk associated with future data use. Second,

when people have some experience in interacting with a private company or perceive it as having a good reputation, they trust the company more (e.g., Appendix 5, with Greek participants).

Responsibility. The responsibility for data misuse (Table 7) appears as another main focus of concern and involves three main actors: the participants themselves, the companies handling the data, and the state that should protect its citizens. The two first are of the greatest concern in participants' eyes (e.g., Appendix 5, with French participants). Some participants added that parents are responsible for ensuring that their children do not give out too much or overly sensitive data, especially on social networking sites.

Table 5. Protection and regulation

Opinions about protection and regulation		**Gender**	**Country**	**Age Range**	**Chi-square**
Need for regulation	'My expectation would actually be that there are very clear legal guidelines for the use of such surveillance cameras.'	M	Germany	25-44	21
Power imbalance	'That's the problem, they're always legally covered. Lawyers aren't stupid. That's why they write these endless pages because they want to insure themselves against everything. But if protection were greater, we probably wouldn't be sitting there.'	M	Germany	15-18	44
No security	'Anyway there's no miracle protection on the Internet. You can use all the firewalls and antiviruses you like, it doesn't do any good.'	M	France	19-24	12
Redress	'I'm thinking of filing a complaint next time. If they ask me for my phone number again, I'll say I am not giving it because your phone calls are causing a disturbance. What right do I have?'	F	Greece	25-44	11
Self-protection	'Not to register is the best protection.'	M	Estonia	19-24	13

Table 6. Trust

Opinions about trust		**Gender**	**Country**	**Age Range**	**Chi-square**
No perceived risk	'But if I give you my bank account number so that you can transfer some money into it, what's the risk in that? You can't access my account.'	F	Poland	19-24	37
Trust, experience and reputation	'That should be a specialist company, a good IT company that has already done something like this and that you trust'	F	Greece	19-24	10 ($p<1\%$)

Table 7. Responsibility

Opinions about responsibility		Gender	Country	Age Range	Chi-square
Self	'It's up to each person to say I'm going to make my Facebook private, I'm going to post this photo, I want to send this photo to everyone and it's up to each person to be responsible.'	M	France	19-24	17
Companies	'Because the provider is responsible and not the state. The state can't always be everywhere and say don't do that.'	M	Germany	15-18	24
State	'I think everyone is responsible. But in a way the state should protect your data, once they're made public. But if you disclose them in the Internet yourself, then it's also your own fault. Then the state can't do anything about it.'	F	Germany	15-18	21
Parents	'We are in a society where transparency prevails over the rest.... There is no longer any limit. We can notice it with the relationship the young people have with the Internet, I can see it at my work. There is no prevention from the parents.'	F	France	45-60	28

These four main privacy-related foci—control, protection and regulation, trust, and responsibility—are particularly useful for clarifying how people make decisions about whether to disclose their personal data to public or private entities. The control issue (Table 4) is influential; people worry about the possible loss of control and misuse of their data. They thus look for any sign that could offer them a guarantee of some control over their data. Most people also ask for more protection, especially through public regulation, though they broadly adopt self-protective behaviours (Table 5). The significant role of trust in online interactions and relationships (Fukuyama, 1996) is confirmed as well (Table 6). People disclose when they trust, which implies that trust is an antecedent of disclosure intentions (Castaneda & Montoro, 2007). Finally, responsibility matters (Table 7): Most people believe it is up to individuals to be responsible when they choose to disclose, even if other entities have some responsibility as well. Although this finding confirms a previous result (Dwyer, 2007), it also is complementary, in that at least some people consider responsibility shared with other entities (e.g., companies, regulators, parents), especially with companies that collect and use data.

Despite consistent support for the importance of these four foci of concerns across all the focus groups, the emphasis on each of them differs, depending on the native country and age of the participants. To test our hypotheses, we therefore ran two correspondence factor analyses (CFA) with country and age variables to identify any cultural and/or generational divides in Europeans' privacy concerns and related behaviours.

Country analysis: Looking for a cultural divide

In Table 8, we present the main topics (lexical worlds) discussed in each country (Alceste software). For example, only three main topics come up in Poland, whereas there are six in Estonia. The percentages listed in each cell indicate the classified CUs in each class and for each country, which implies the importance of each topic. For example, Germans focused a lot on security and monitoring, a subject that appears in approximately 44 percent of the sentences.

Table 8. Main lexical worlds in each of the seven countries studied

Germany (4 classes)	**France (4 classes)**	**Greece (5 classes)**	**Spain (5 classes)**	**Poland (3 classes)**	**Romania (4 classes)**	**Estonia (6 classes)**
Data disclosure (20%)	Data disclosure, use, & regulation (16%)	Data disclosure & data use (21%)	Trust & control (12%)	Control & regulation (70%)	Privacy & relationships (15%)	Data use & risks (11%)
Protection & responsibility (13%)	Responsibility (15%)	Data use, protection & redress (24%)	Mandatory disclosure & regulation (11%)	Data disclosure (22%)	Data access & consent (13%)	Anonymity (14%)
Conditions of data disclosure (23%)	Risks & dangers (26%)	Data use & consent (11%)	Social networking (9%)	Authentication & security (8%)	Monitoring & regulation (22%)	Protection strategies (18%)
Security & monitoring (44%)	Privacy invasion (43%)	Trust & control (12%)	Virtuality (33%)	—	Data disclosure (50%)	Experience & trust (24%)
—	—	Identification (32%)	Monitoring & privacy invasion (35%)	—	—	Public data (19%)
—	—	—	—	—	—	Passwords (14%)

Table 8 highlights the similarities and differences in the main topics focused on in each country:

- Data disclosure is a matter of public concern in all countries, though in Estonia, the discussion centred more on data that can be made public.
- Issues of control, protection, and regulation were debated in all countries; the analysis highlights particularly the importance of control and the absence of secure protection.
- The issue of trust and control appears as a specific lexical world for two Southern countries (Greece and Spain).
- Responsibility appears mainly in Germany and France (i.e., Old Europe). In France, it appears as a specific lexical world.

Overall, these results reinforce Dinev and Hart's (2006) argument that data uses are a prime concern and that a lack of individual control over data creates privacy anxiety. However, we also find that these universal issues emerge differently in the various European countries, with emphases on specific foci, depending on the country considered. Such divergences reflect varying historical experiences, economic development, and political/cultural situations (Howard & Mazaheri, 2009). For example, Eastern Europe lagged behind Western Europe in terms of IT development for many years but has progressed very quickly in the twenty-first century (Kornai, 2006). E-commerce as a proportion of total commerce in Poland doubled during 2004–2006 (Polasik & Wisniewski, 2009), which likely explains the importance of control and regulation issues in this country. Estonia is pioneering e-government and e-democracy (Madise & Martens, 2006), and the implementation of a sophisticated, mandatory eID card in this country may explain concerns about public data, identification, and authentication. Our results also support Colesca and Dobrica's (2008) claim that trust is a key determinant of e-government adoption in Romania; we add the importance of informed choice, control, and monitoring. Whereas Panopoulou et al. (2009) conclude that e-government participation is not a common practice in Greece and Spain, we find that control over data use is the biggest concern in these countries, though in Spain, hostility to government monitoring also may be influential. Consent and choice thus must be highlighted to encourage online participation there.

In Old Europe, we find no consensus about which entities are responsible for promoting Internet security and privacy, a topic that has rarely been a focus of previous privacy research. This result parallels Marsden's (2008) discussion of the blurred lines among individuals, companies, and governments in terms of security governance. Our findings offer a complementary view by suggesting that a range of perspectives describe individual and collective responsibility for data privacy, possibly due to varying perceptions of the relationship between the individual and the state, which runs through discussions of public/private organizations, regulation, and responsibility. We believe that historical/political factors also play a role here, as suggested by Howard and Mazaheri (2009).

Research on privacy has recently considered social networks (e.g., Boyd & Ellison, 2007), but this topic did not emerge as a major theme in our study. The risks most discussed by our focus group participants instead were criminal actions, such as financial fraud and identity theft, suggesting heightened awareness of organized crime online (Anderson & Moore, 2009). This perception also sheds some light on why the rule of law acts as a predictor of national differences in Internet usage across Europe (Orviska & Hudson, 2009).

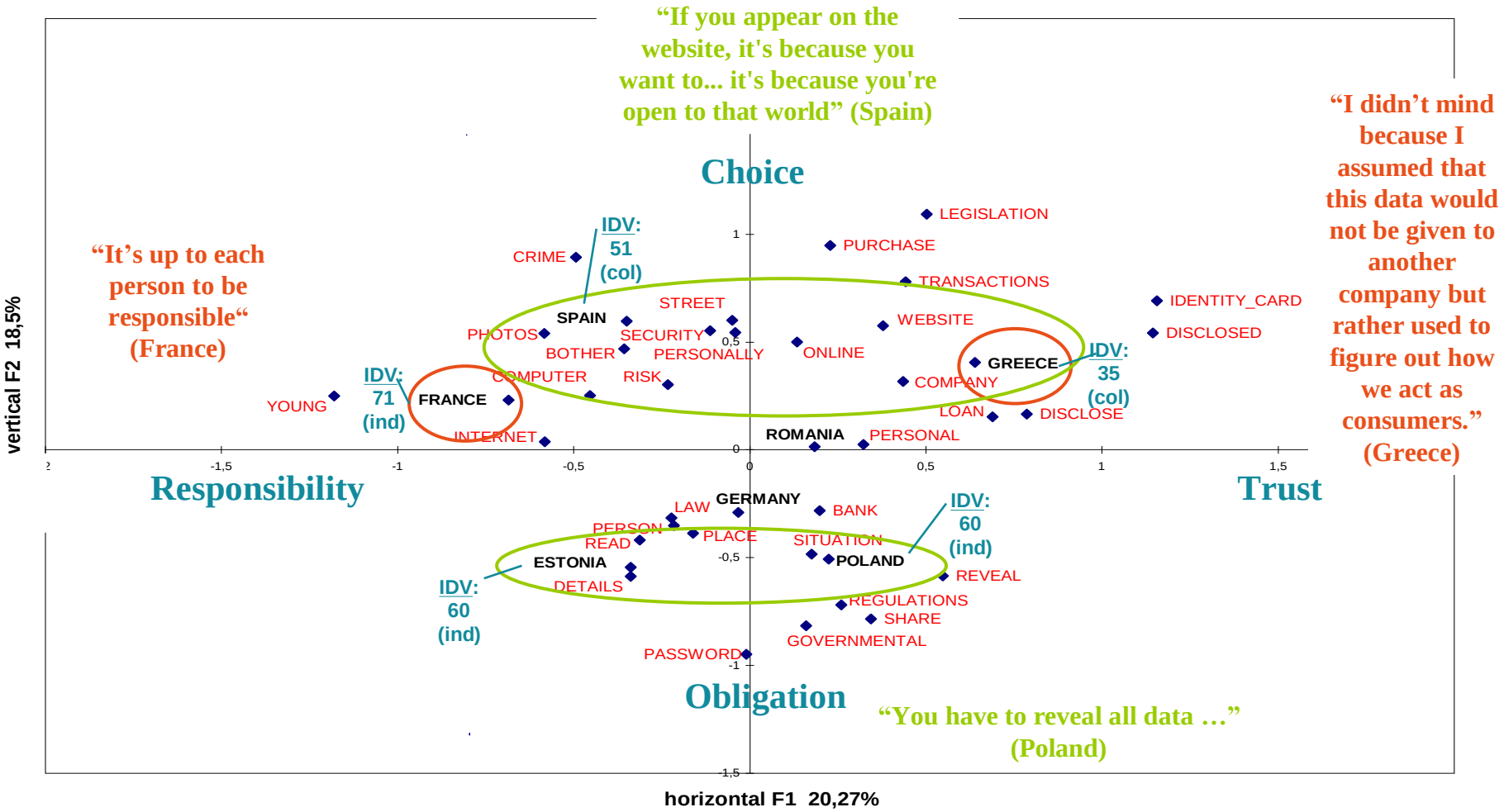
To confirm these preliminary results, we present our WordMapper CFA analyses and summarise them, especially the similarities and differences across the seven countries, in Figure 2. The words most frequently employed in each country appear next to each nation's name. To develop this graph, the program produces, for each word and variable value (i.e., country) the absolute and relative contributions (to each axis) and coordinates. The first two axes explain 20.27 percent and

18.50 percent in the level of inertia, or 38.77 percent in total. Romania and Germany appear in the middle of the graph, because they cannot be differentiated on the two first axes.

In Figure 2 we find a clear opposition on axis 1 between France (Old Europe, left side), which underlines the importance of responsibility, and Greece (South, right side), which focuses on trust. These findings are coherent with the Alceste results, (Table 8), in which responsibility emerged as an important topic for France but trust appeared unimportant, and the results were reversed for Greece. This outcome reflects differences in the level of Internet use, which is very low in Greece (31%)—such that people's lack of knowledge and experience emphasise the need for trust—but significantly higher in France (62%), such that people are more conscious of their responsibilities. This gap is also reflected in opposing positions on regulation and the role of public bodies. Greek participants regard authorities as an important means of protection ('*the legislation, that is what defines each side's rights and obligations'*), whereas the French welcome public intervention but are sceptical about whether current regulations really work ('*the CNIL [French data protection authority] must intervene to do its job, that is, to take every file to work on it'*).The divide can also be explained by the individualism–collectivism dimension of national culture: Greece is a more collectivist national culture (IDV = 35) than France (IDV = 71). That is, people in collectivist countries appear to trust more and are more willing to self-disclose, as indicated by Posey et al. (2010) and in support of our first hypothesis.

The factorial analysis per country also reveals an opposition on the second axis between the two Southern countries (top of the graph) and both Eastern countries, one from the second block and one from the first block (bottom of the graph). This opposition indicates whether respondents express the belief that they have some choice about whether to reveal personal data (Greece and Spain) or if they perceive a lack of choice (Poland and Estonia), such that they are 'forced' to give their data to trusted institutions (e.g., banks, governments, well-known companies) but reluctant to offer them to other organizations. This gap is well illustrated by a Polish participant: '*With governmental organizations, I simply do that because I have to, I don't think about whether it is necessary or not'*. Polish participants clearly differentiate trustworthy organizations from those that cannot be trusted, whereas the Spanish focus group members think they have to trust the government at least: '*If we can't trust the government, who can we trust? We've got to trust someone, don't we?*' This result confirms the importance of considering the forced consent dimension in an online context. Without full awareness, consumers cannot be said to give their consent freely. This cultural divide between southern and eastern countries reflects individualism–collectivism opposition too: Greece (IDV = 35) and Spain (IDV = 51) are collectivist countries, where people trust and disclose more, whereas Poland and Estonia (IDV = 60) are individualist societies, where people are reluctant to disclose and feel compelled to do it, in line with our first hypothesis. These results match findings by Milberg et al. (2000), Steenkamp and Geyskens (2006), and Posey et al. (2010) and contribute to the debate on the influence of the individualism–collectivism dimension of national culture on disclosure behaviours.

Figure 2. Factorial map per country: Cultural similarities and differences in seven EU countries regarding privacy issues



Age analysis: Generational divide

In Figure 3, we depict the most frequently employed words by age category. The two axes explain 36.39 percent and 26 percent of the inertia. The first axis contrasts the views of respondents aged 45 to 60 years (left side) with those of respondents younger than 25 years (right side). The second axis contrasts the 45–60-year cohort (bottom) with the young adults group (25–44 years) (top). The absolute contribution of the older group (more than 61 years old) is very low on each axis.

Middle-aged people (45–60 years) have rather negative views about data disclosure and use, perceiving many risks that are difficult to prevent. Younger people (19–24 years mainly) are more positive, feel more responsible, and are more confident of their ability to prevent possible data misuse, such that: '*when you use the Internet you know perfectly well everybody is going to have access to what you do and we've also got access to what other people do. But that's what it's about, it's the way it works. And then you abide by the rules'*. On axis 2, the same opposition appears between middle-aged people who fear privacy invasions and the younger adults (25–44 years) who take an intermediate position, not really confident but not untrusting either: '*we at least have a way to ask: "hey, that data, where did it come from?" and if we don't find out we can at least demand responsibilities from whoever sold our data'*.

These results indicate that young people express fewer privacy concerns than adults as already suggested by Moscardelli & Liston-Heyes (2004) and Palfrey & Gasser (2008). Few previous empirical studies have demonstrated this finding conclusively however. Our work therefore offers an interesting empirical test of this tendency. In our study, 18.5 percent of the participants younger than 25 years declared themselves unconcerned by privacy, whereas that status was true of only 8.1 percent of older participants. These observations are also coherent with Hoofnagle et al.'s (2010) recognition that higher proportions of 18–24-year-olds believe incorrectly that the law protects them.

The young people's confidence in legal protections does not prevent them from feeling responsible for their own protection. In line with previous results from Lenhart and Madden (2007) and Moscardelli and Divine (2007), we show that young people are more likely than adults to post fake information, as illustrated in a comment from a 19–24-year-old participant: '*we give our personal details, but only those which we consent to reveal. My first account at Nasza-Klasa was fictitious. I pretended to be someone I wasn't. I didn't know how it all worked, so I remained anonymous. Later I thought I could reveal some more because I might have better contact with others'.* Using the survey participants filled in before the discussion, we determined that this habit is less common among adults (47.5% of participants aged 19–24 years said they used a pseudonym, compared with 21.7% of participants aged 25–44 years and 33.3% of those aged 45–60 years).

In addition to the cultural divide, there is thus a clear generation divide, such that for privacy issues, younger generations are more responsible and confident than older adults, which supports our second hypothesis. This finding is in line with some results in prior literature that show that young

people are more self-confident Internet users, as 'digital natives' (Baumann, 2010). However, our results also contradict conventional 'scare-mongering' about young people's online lives (Herring, 2008), which depicts them as reckless and ignorant. Instead, young people take a greater degree of personal responsibility, perhaps because their relative technological expertise allows them to do so. This more nuanced picture of young people portrays them as active agents, engaging with privacy in different ways than their parents, but not lacking in concern about access to and control of their personal data. These findings reveal a reversed privacy paradox for young people: lower privacy concerns combined with a greater use of protection strategies. We thus contribute to the controversy regarding privacy concerns among young people and adults (as illustrated in Table 1). Studies that indicate greater privacy concerns among young people refer to their use of protection behaviours; we suggest that low privacy concerns can combine with high protection strategies, which clarifies the consequences of young people's privacy concerns on protective behaviours instead of risky ones.

In summary, the decision to disclose personal data to public or private entities relies on four main privacy-related concerns (i.e. control, protection, trust, and responsibility) that offer important decision criteria and can help explain differences in disclosure and protection behaviours. Our findings also are in line with our two main hypotheses. First, people from different countries in Europe differ in their privacy concerns and declared behaviours, such that those from collectivist countries express more trust and are less reluctant to disclose information than are those from individualistic countries, in support of H1. Second, a clear generational divide appears, in which young people have a more positive view of personal data management than older people, are more confident in law protection and in their own ability to protect themselves, and sometimes engage in specific behaviours for protection, such as lying. This finding offers support for H2 as well.

On the basis of the focus group results, we developed a theoretical model (Figure 4) to capture the various aspects of users' privacy-related concerns and consequences on their subsequent behaviours. For example, this model suggests that the way in which people see and understand responsibility in regards to data handling could at least partly influence their privacy concerns and subsequent behaviours in terms of data disclosure and protection. Whether people consider it is part of their responsibility to take care of how their personal data could be used in the future or give this responsibility to companies collecting the data or to data protection authorities should indeed clearly influence how and to which degree they would consider themselves as concerned by their privacy. The same holds true for the other three privacy-related foci of concern presented in our model.

This model partly echoes one recent study which considers that 'perceived information control and perceived risk are salient determinants of perceived information privacy' (Dinev et al. 2013, p. 295). We confirm here the salient influence of control while completing the list of determinants of privacy concerns by adding also trust, perceived protection and regulation as well as perceived responsibility.

Figure 3. Factorial map per age: Generational similarities and differences regarding privacy issues

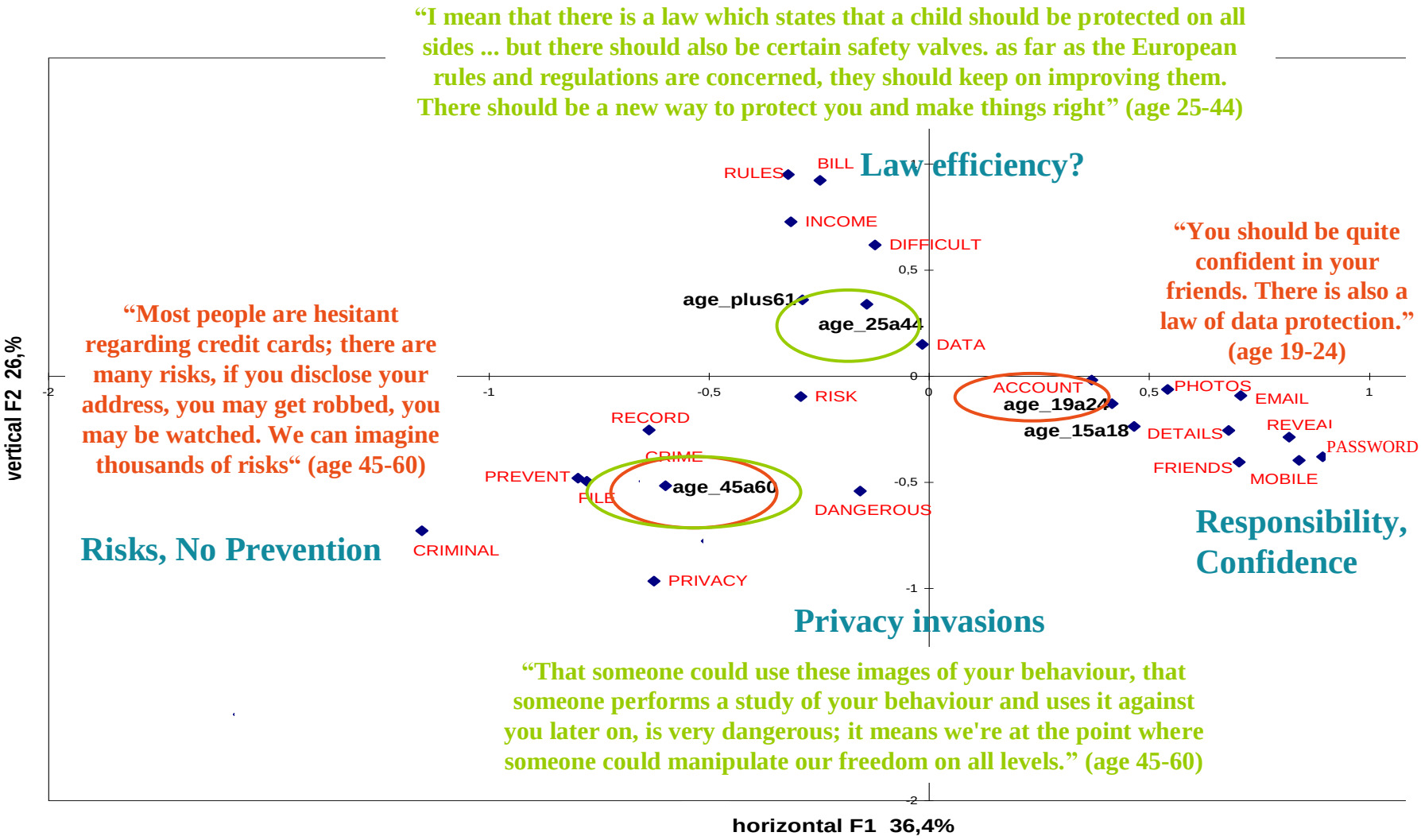
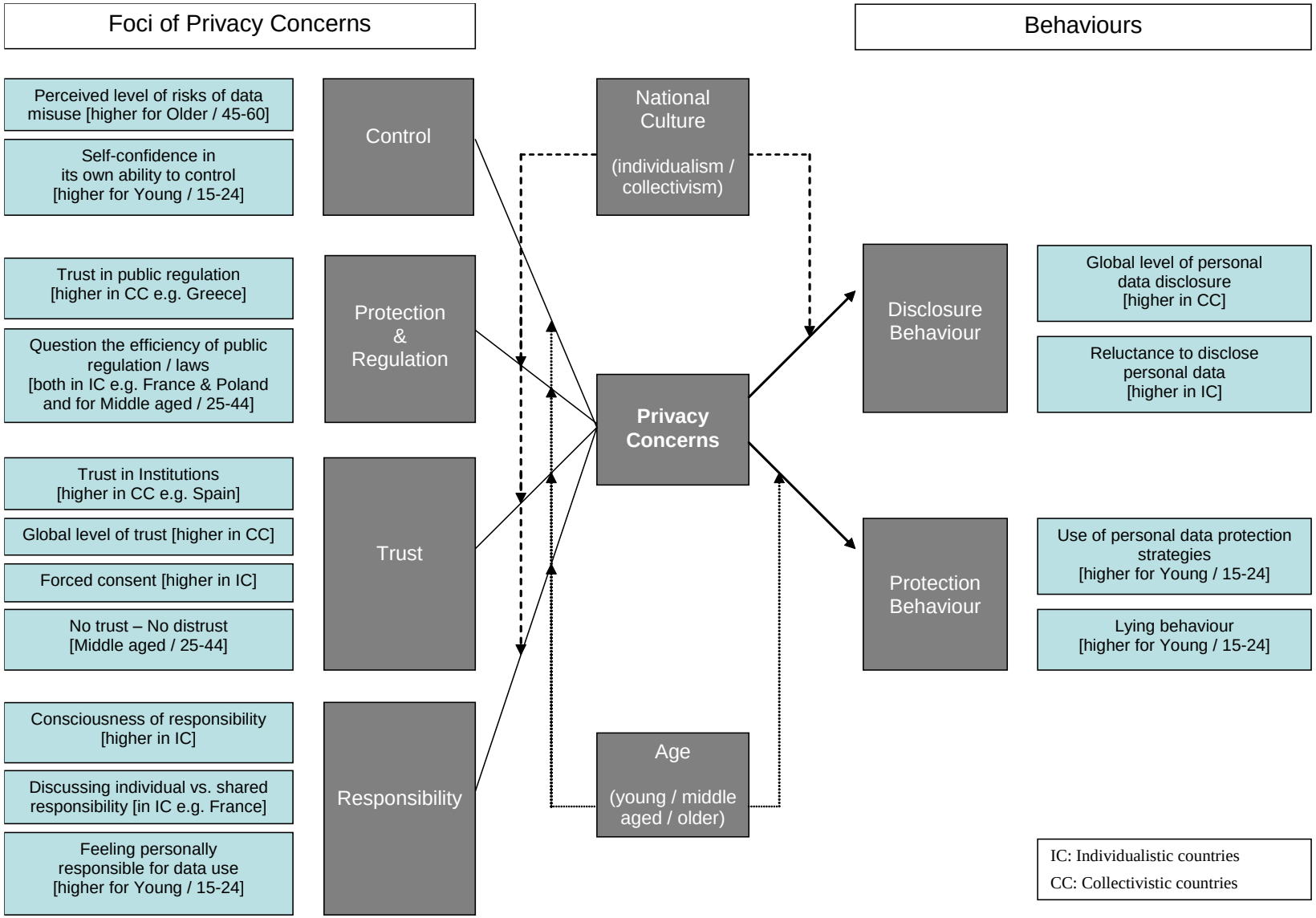


Figure 4. Summary of focus group results and proposed research model



The framework in Figure 4 also suggests the potential influence of both the national culture and the age of the person as potential moderators of the proposed relationships. It should be noted that, given our results, culture mostly seems to influence and moderate the relationship between privacy concerns and disclosing behaviours whereas age mostly moderate the relationship with protecting behaviours. Although the influence of age and culture has already been studied in previous literature, we offer here a more comprehensive picture of what is really going on, in particular as regards the potential different moderating effects of these two variables on the relationship between privacy concerns and both disclosure and protection behaviours.

Discussion

Our results provide major theoretical, methodological, and policy implications. From an academic perspective, this article is one of the few contributions to privacy literature that comes from a qualitative angle to learn more about privacy issues from the perspective, and the words, of European citizens themselves. This extension to extant literature goes beyond the confines of a positivist standpoint or American and student samples. Although some of the foci of privacy concerns that emerge from our results, including lack of control and protection, have been identified in previous literature, they rarely appear in combination. Our results offer a more profound consideration of the various issues that worry European citizens and support a detailed assessment of the similarities and differences in people's attitudes and behaviours, depending on both their country of origin and age.

Our study depicts a detailed picture of issues of shared concern for Europeans, such as data control, and where their ideas diverge, such as the balance of trust and responsibility. It also indicates how people make the decision to disclose (or not) their personal data, which is still a major question, considering the prior contradictory results in previous literature. The model we propose as a synthesis of our results offers new research opportunities for further quantitative studies in this area.

One key theoretical contribution of this work pertains to the discussion of perceived responsibility in data handling, an area that has rarely been studied in previous privacy literature, despite its importance. This central issue could both influence the choice of data protection strategies and explain some troubling privacy paradoxes in consumer behaviours. Concerns about shared responsibility appear especially interesting, considering people's differing feelings of trust toward the multiple entities involved in data collection, use, and protection. For example, most participants reported a lack of trust toward some private companies, which raises questions about how to create and cultivate trust in companies' personal data handling practices. In addition, increasing regulation may not be an automatic route to greater trust because many people call for more regulation but also express distrust in its implementation. Thus, doubts about public authorities' ability to regulate personal data must be addressed if regulatory confidence-building measures are to succeed.

From a methodological point of view, we undertook qualitative research through 14 focus groups. With our good sample size and diversity (seven countries, 139 participants who vary in gender, age,

and professional status), we validate the existence of both cultural and generational divides through a statistical analysis of textual data. This approach offers added value over manual textual analyses, which often require laborious assignments of codes to sections of text to ascertain meaning from a mass of material. Our categories are based less on suppositions of meaning and more on word counts and relationships within the text (Marchand, 2007). This approach is particularly useful in this study, considering the size of the corpus. Although widely used in psychology, sociology, and political sciences, this method is less common in management science and information systems research; our findings indicate its potential benefits for the field. We used different methods to ensure both the validity and the reliability of the results, including triangulation with participants from different backgrounds, ages, and countries; two investigators; two statistical analysis methods (DHC and CFA); and two software packages (Alceste and WordMapper). The findings reveal the complementarity of our methods and software, as well as the convergence of the results, which confirms the importance of triangulation to ensure the quality of qualitative data results.

Finally, we show that it is possible to explore key strands of the debate that continues in European and national policy settings in significant depth. Recent reports raise concerns about privacy invasions (e.g., Lusoli & Miltgen, 2009); our results show how to determine the importance of these issues for European people, which in turn can reveal whether a new regulatory framework is required. This work thus has great relevance for public policy questions about online data, which have become urgent to solve for the EU and national governments.

Limitations and further research

Our results are not without limitations, which offer interesting opportunities for further research in this area. The first limitation involves our use of only one country in the first block (Northern Europe). Further research should compare these results with findings obtained in Nordic countries (e.g., Denmark, Finland, Norway) or a country that has recently joined the EU, such as Latvia or Lithuania.

Our qualitative study focused mainly on people's perceptions, attitudes, and opinions; it does not test the hypotheses in a traditional sense or prove causal links among the interesting concepts, as would be possible with survey data. If the results are not statistically generalisable to all people and settings though, they are generalisable to the theoretical propositions (analytic generalisation). Therefore, to extend our findings, we recommend a quantitative approach that tests the proposed model with a larger sample of European and non-European people.

We developed careful English translations of the discussions, to compare the discourses from the different nations, but doing so meant we could not take language specificities into account. Although very difficult to manage, a further analysis of the discussions in their original languages could offer a richer understanding of the specificities of the different cultures.

As we noted previously, Hofstede's model of national culture has some limitations that continuing research must address. Culture is notoriously difficult to define and conceptualise (Boyacigiller et al.,

1996); establishing a measure that can correctly gauge the distance between cultures represents a constant challenge (Shenkar, 2001). Critiques of Hosftede's approach (e.g., Sondergaard, 1994; Smith et al., 1996b) note that (1) culture does not equate to nations, (2) it is to difficult to understand culture through numerical indices and matrices, (3) there is little confidence in the assumptions of stability of cultural differences, (4) a lack of independence in the units of analysis is suspected but not incorporated in the calculation of the indices (Baskerville, 2003), and (5) the presumption that everyone within a given national culture fits within a simple polarity is questionable (Ess & Sudweeks, 2005). Yet these criticisms have not diminished the attractiveness of Hosftede's indices; his model of national culture is widely used (Baskerville, 2003). Many authors demonstrate compellingly that Hofstede's model functions well for at least some kinds of online research (Ess & Sudweeks, 2005) and that the predicted cultural differences generally can be confirmed (Ryan et al., 1999). In addition, studies that have not explicitly used Hofstede's paradigm often return similar dimensions (e.g., Lytle et al., 1995). However, more studies could use alternative models of culture, such as the GLOBE framework (House et al., 2004; cf. Grinstein, 2008). A common criticism of Hofstede's model, namely, that it measures culture at a macro (country) level and lacks precision at the micro (individual) level, also might be addressed by methods that assess cultural traits at the individual level of analysis using personality tests (Srite and Karahanna 2006), responses to specific cultural values embedded in scenarios (Straub et al. 2002), or scores on the CVSCALE (Donthu & Yoo, 1998; Patterson et al. 2006). Such alternatives can offer fruitful contributions, but they suffer their own potential drawbacks (Oyserman et al. 2002). Therefore, a rigorous assessment of all the cultural identifiers of each individual in a sample would best complement and improve the internal validity of our results.

Our findings indicate the tendency of young people to be less concerned than adults about privacy issues and predisposed to protecting themselves by giving false information. This result can be explained by some specific features of young people, such as their greater risk propensity, which is a central element of adolescents' identity construction (Hope, 2007). Although our epistemological position made it impossible to test this assumption, it remains an interesting issue for future studies.

In their recent study, Dinev et al. (2013) found empirical support that perceived information control and perceived risk shape an individual's perceived privacy. Our study confirms the significant influence of control but find trust, instead of risk, as a salient determinant of privacy. In addition, although Dinev et al. (2013) consider regulatory expectations as a determinant of risk, we find protection and regulation as a direct determinant of privacy. We finally add perceived responsibility as a fourth important privacy-related determinant. Further study should inform which of these criteria are direct or indirect determinants of privacy, whether it is trust, risk or both which shape an individual's perceived privacy and whether these processes are similar or different between national cultures. It may be, indeed, that trust matters more in some countries whereas risk is a more important determinant in other countries.

Finally, citizens of different European nations vary in their privacy fears and ideas about how to assuage these fears; these variations appear likely to persist. As e-identification becomes a more

pervasive part of European life, further research is needed to help citizens, companies, and governments make better decisions about their mutual roles in online privacy protection (Lusoli & Miltgen, 2009). This balance of responsibility demands further investigation to clarify why Europeans have such strong and divergent views about how citizens, companies, and governments should interact to protect online privacy. Additional research in this area should also address the identification, classification, and measurement of the factors that influence Internet users' attitudes toward security and privacy issues.

Conclusion

This study highlights four main foci of privacy concerns (control, protection and regulation, trust, and responsibility) that appear to influence the decision to disclose personal data. Confirming the importance of data use and control, this research pinpoints the relevance of the hotly contested issue of responsibility for personal data management. In addition, some key cultural and generational differences appear, including a north–south divide regarding the significance of responsibility versus trust. Issues of control and choice also prompt different perceptions: In the south, people believe they have a choice, whereas in Eastern Europe, people believe they are forced to disclose. In relation to age, young people feel more positive, more responsible, and more confident of their ability to prevent possible data misuse, and they trust the efficiency of legal protection more than adults do. A reverse privacy paradox thus appears in our results: The lower privacy concerns of young people combine with their higher protective behaviours to offer an explanatory framework for contradictory results in prior literature pertaining to their level of privacy concerns, factors influencing this level, and consequences in terms of their behaviours.

References

ALLIK J and REALO A (2004) Individualism-collectivism and social capital. *Journal of Cross-Cultural Psychology 35* (January), 29-49.

ANDERSON R and MOORE T (2009) Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society* 367 (1898), 2717-2727.

ASBURY J (1995) Overview of focus group research. *Qualitative Health Research* 5, 414-420.

BA S and PAVLOU PA (2002) Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premium and Buyer Behavior. *MIS Quarterly* 26 (3), 243-268.

BAIER A (1986) Trust and antitrust. *Ethics* 96, 231-260.

BANSAL G, ZAHEDI F and GEFEN D (2008) *The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation*. 29th International Conference on Information Systems, Paris, France, December 14-17.

BANSAL G, ZAHEDIB FM and GEFEN D (2010) The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems* 49(2), 138-150.

BASKERVILLE RF (2003) Hofstede Never Studied Culture. *Accounting, Organizations and Society* 28, 1-14.

BAUMANN M (2010) Pew report: digital natives get personal. *Information Today* 27 (10).

BÉLANGER F and CROSSLER RE (2011) Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35 (4), 1017-1041.

BELANGER F, HILLER JS and SMITH WJ (2002) Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems* 11 (3-4), 245-270.

BELLMAN S, JOHNSON EJ, KOBRIN SJ and LOHSE L (2004) International differences in information privacy concerns: a global survey of consumers. *The Information Society* 20(5), 313-324.

BENNETT CJ (1992) *Regulating Privacy: Data Protection And Public Policy In Europe And The United States*, Ithaca, NY: Cornell University Press.

BENZECRI JP (1981) *Pratique de L'Analyse des Données, Linguistique et Lexicologie*. Dunod, Paris.

BLOMQVIST K (1997) The many faces of trust. *Scandinavian Journal of Management* 13 (3), 271-286

BOYACIGILLER N, KLEINBERG MJ, PHILIPS M and SACKMANN S (1996) Conceptualizing Culture. In *Handbook for international Management Research* (PUNNETT BJ and SHENKAR O), MS: Blackwell, Cambridge.

BOYD DM (2007) Why Youth (Heart) Social Network Sites: The Role of Networked Publics. In *Youth, Identity and Digital Media* (BUCKINGHAM D, Ed), 119–142, MIT Press, Cambridge, MA.

BOYD DM and ELLISON NB (2007) Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13 (1), 210-230.

BURCHELL S, CLUBB C, HOPWOOD AG, HUGHES J and NAHAPIET J (1980) The Roles of Accounting in Organizations and Society. *Accounting, Organizations, and Society* 5(1), 5-27.

CASTANEDA JA and MONTORO FJ (2007) The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research* 7(2), 117-141.

CAVERLEE J and WEBB S (2008) *A large-scale study of MySpace: Observations and implications for online social networks*. In 2nd International Conference on Weblogs and Social Media (AAAI).

CLARKE R (1999) Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM* 42 (2), 60-67.

COLESCA SE and DOBRICA L (2008) Adoption and use of e-government services: the case of Romania. *Journal of Applied Research and Technology* 6(3), 204-217.

CONSUMERS-UNION (2008) Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy, September 25, Available at: http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

CULLEN R (2009) Culture, identity and information privacy in the age of digital government. *Online Information Review* 33(3), 405-421.

CULLEN R and REILLY P (2007) Information privacy and trust in government: a citizen-based perspective from New Zealand. *Journal of Information Technology and Politics* 4(3), 61-80.

CULNAN M and ARMSTRONG P (1999) Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation. *Organization Science* 10 (1), 104-115.

COX KK, HIGGINBOTHAM JB and BURTON J (1976) Applications of Focus Group Interviews in Marketing. *Journal of Marketing* 40 (1), 77-80.

DAVISON RM, CLARKE R, SMITH HJ, LANGFORD D and KUO B (2003) Information Privacy in a Globally Networked Society: Implications for IS Research. *Communications of the Association for Information Systems* 12 (22), 341–365.

DELONG DW and FAHEY L (2000) Diagnosing Cultural Barriers to Knowledge Management. *Academy of Management Executive* 14(4), 113-127.

DIETZ G, SKINNER D and WEIBEL A (2011) *The true dark side of trust: when trust becomes a 'poisoned chalice'*. In Proceedings of the Academy of Management Annual Meeting, 2011.

DINEV T and HART P (2006) Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce* 10(2), 7-29.

DINEV T, MASSIMO B, HART P, RUSSO V and COLAUTTI C (2006) Privacy calculus model in e-commerce - a study of Italy and the United States. *European Journal of Information Systems* 15(4), 389-402.

DINEV T, XU H, SMITH JH and HART P (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* 22, 295-316.

DONTHU N and YOO B (1998) Cultural influences on service quality expectations. *Journal of Service Research* 1 (2), 178-186.

DWYER C (2007) *Digital relationships in the ''MySpace'' generation: Results from a qualitative study*. In Proceedings of 40th Hawaii International Conference on System Sciences, Big Island, Hawaii, IEEE, Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4076409&isnumber=4076362

EASTLICK MA, LOTZ SL and WARRINGTON P (2006) Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research* 59(8), 877-886.

ESS C and SUDWEEKS F (2005) Culture and computer-mediated communication: Toward new understandings. *Journal of Computer-Mediated Communication* 11(1), article 9. Available at: http://jcmc.indiana.edu/vol11/issue1/ess.html

FERN EF (1982) The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality. *Journal of Marketing Research* 19, 1-13.

FOGEL J and NEHMAD E (2009) Internet social network communities: Risk taking, trust, and

privacy concerns. *Computers in Human Behavior* 25(1), 153–160.

FRIEDMAN B, KHAN Jr. PH and HOWE D (2000) Trust online. *Communications of the ACM* 43(12), 34-40.

FUKUYAMA F (1996) *Trust: The Social Virtues and the Creation of Prosperity*. Simon and Schuster, New York.

GEPHART R (2004) Qualitative research and the Academy of Management Journal. *Academy of Management Journal* 47(4), 454-462.

GOVANI T and PASHLEY H (2007) *Student awareness of the privacy implications when using Facebook*. Carnegie Mellon University. Available at: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf.

GRINSTEIN A (2008) The effect of market orientation and its components on innovation consequences: a meta-analysis. *Journal of the Academy of Marketing Science* 36 (2), 166–173.

GROSS R and ACQUISTI A (2005) *Information revelation and privacy in online social networks*. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society - *WPES '05.*

GUBA EG and LINCOLN YS (1981). *Effective evaluation: Improving the usefulness of evaluation results through responsive and naturalistic approaches*. Jossey-Bass, San Francisco, CA.

HERRING SC (2008) Questioning the Generational Divide: Technological Exoticism and Adult Constructions of Online Youth Identity. In *Youth, Identity, and Digital Media,* pp 71-92, Massachusetts Institute of Technology.

HOFSTEDE G (1980) Culture's Consequences: International Differences. In *Work-Related Values*, pp 335-355, Sage Publications, Beverly Hills, CA.

HOFSTEDE G (1991) *Culture and Organizations: Software of the Mind*. McGraw Hill, London.

HOOFNAGLE C, KING J, LI S and TUROW J (2010) How different are young adults from older adults when it comes to information privacy attitudes and policies, available at: http://ssrn.com/abstract=1589864.

HOPE A (2007) Risk Taking, Boundary Performance and Intentional School Internet "Misuse". *Discourse: Studies in the Cultural Politics of Education* 28 (1), 87-99.

HOUSE RJ, HANGES PJ, JAVIDAN M, DORFMAN P and GUPTA V (2004) *Culture, Leadership, and Organizations: The GLOBE Study of 62 Societies*. Sage Publications, Thousand Oaks, CA.

HOWARD PN and MAZAHERI N (2009) Telecommunications Reform, Internet Use and Mobile Phone Adoption in the Developing World. *World Development* 37 (7), 1159-1169.

IBM (1999) *IBM multi-national consumer privacy survey*. Somers, NY: IBM Global Services, October. http://www.ibm.com/services/files/privacy survey oct991.pdf

JAVIDI M, LONG LW, VASU ML and IVY DK (1991) Enhancing focus group validity with computer-assisted technology in social science research. *Social Science Computer Review* 9, 231-245.

JOHNSON J (1992) A Theory of the Nature and Value of Privacy. *Public Affairs Quarterly* 6 (3), 271-292.

JONES S, JOHNSON-YALE C, MILLERMAIER S and PEREZ FS (2009) Everyday life, online: U.S. college students' use of the Internet. *First Monday* 14(10). Available at: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2649/2301

KAGITCIBASI C (1997) Individualism and Collectivism. In *Handbook of Cross-Cultural Psychology: Social Behavior and Applications*, Vol. 3 (BERRY JW, SEGALL MH and KAGITCIBASI C, Eds), pp 1-49, Allyn & Bacon, Boston.

KELLY AE and McKILLOP KJ (1996) Consequences of revealing personal secrets. *Psychological Bulletin* 120, 450-465.

KITZINGER J (1995) Introducing focus groups. *British Medical Journal* 311, 299-302.

KORNAI J (2006) The great transformation of Central Eastern Europe. *Economics of Transition* 14, 207–244.

KRASNOVA H, HILDEBRAND T and GUENTHER O (2009) *Investigating the Value of Privacy in Online Social Networks: Conjoint Analysis*, in Proceedings of the 30th International Conference on Information Systems, Phoenix, AZ, December 15-18.

LAMPE C, ELLISON N and STEINFIELD C (2008) *Changes in use and perception of Facebook*. In Proceedings of the ACM conference on Computer supported cooperative work, 721–730.

LEBART L and SALEM A (1994) *Statistique Textuelle*. Dunod, Paris.

LEIDNER DE and KAYWORTH TR (2006) A Review of Culture in Information Systems Research: Toward a Theory of Information Technology Culture Conflict. *Management Information Systems Quarterly* 30(2), 357-399.

LENHART A and MADDEN M (2007) *Teens, Privacy and Online Social Networks*, Washington, DC: Pew Internet & American Life Project. Available at: http://www.pewInternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx

LENHART A, MADDEN M, SMITH A and MACGILL A (2007) *Teens and social media*. Washington, DC: Pew Internet & American Life Project.

LI Y (2011) Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems* 28 (28), 453-496.

LIFE SUPPORT (2010) *Young people's needs in a digital age*, available at: http://eryica.org/files/Life%20Support-%20Young%20people%27s%20needs%20in%20a%20digital%20age.pdf

LIVINGSTONE S (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media Society* 10(3), 393-411.

LUSOLI W and MILTGEN C (2009) *Young people and emerging digital services: an exploratory survey on motivations, perceptions and acceptance of risks*. JRC Scientific and Technical Reports EUR 23765 EN, LUSOLI W COMPAÑÓ R and MAGHIROS I (Eds.), Sevilla: EC JRC IPTS.

LYTLE AL, BRETT JM, BARSNESS ZI, TINSLEY CH, JANSSENS M (1995) A paradigm for confirmatory cross-cultural research in organizational behavior. *Research in Organizational Behavior* 17, 167-214.

MADDEN M, FOX S, SMITH A, and VITAK J (2007) Digital Footprints: Online Identity Management and Search in the Age of Transparency, PEW Research Center Publications, Available at: http://pewresearch.org/pubs/663/digital-footprints

MADISE U and MARTENS T (2006) E-Voting in Estonia 2005. The First Practice of Country-wide Binding Internet Voting in the World. In *Electronic Voting 2006* (KRIMMER R, Ed), pp 15-26, 2nd International Workshop, LNI, 86.

MALHOTRA NK, KIM SS and AGARWAL J (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15 (4), 336-355.

MARCHAND P (2007) Concepts, méthodes et outils. In *Analyse statistique de données textuelles en sciences de gestion – Concepts, méthodes et applications* (GAUZENTE C and PEYRAT-GUILLARD D, Eds), pp 47-70, Editions EMS, collection Management & Société, Paris.

MARSDEN CT (2008) Beyond Europe: The Internet, Regulation, and Multistakeholder Governance—Representing the Consumer Interest? *Journal of Consumer Policy* 31(1), 115-132.

MARWICK AE, DIAZ DM and PALFREY J (2010) *Youth, Privacy and Reputation*. Berkman Center for Internet and Society, Research Publication No. 2010-5, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163.

MASON S (1986) Four ethical issues of the information age. *MIS Quarterly* 10(1), 5-12.

MAYNARD ML and TAYLOR CR (1996) A comparative analysis of Japanese and U.S. attitudes toward direct marketing. *Journal of Direct Marketing* 10(1), 34-44.

MENDES DE ALMEIDA PF (1980) A review of group discussion methodology. *European Research* 8 (3), 114–120.

MERRIAM SB (1998) *Qualitative research and case study applications in education*. Jossey-Bass, San Francisco.

MERTON RK, FISKE M, KENDALL PL (1990) *The Focused Interview*. Free Press, New York.

MERTON RK, KENDALL PL (1946) The focused interview. *American Journal of Sociology* 51, 541-57.

MILBERG SJ, BURKE SJ, SMITH HJ and KALLMAN EA (1995) Values, personal information privacy, and regulatory approaches. *Communication of the ACM* 38(12), 65-74.

MILBERG SJ, SMITH HJ and BURKE SJ (2000) Information privacy: Corporate management and national regulation. *Organization Science* 11(1), 35–57.

MORRIS MG, VENKATESH V and ACKERMAN PL (2005) Gender and age differences in employee decisions about new technology: an extension to the theory of planned behavior. *IEEE Transactions on Engineering Management* 52 (1), 69-84.

MOSCARDELLI DM and DIVINE R (2007) Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships With Privacy-Protecting Behaviors. *Family and Consumer Sciences Research Journal* 35(3), 232-252.

MOSCARDELLI DM and LISTON-HEYES C (2004) Teens Surfing The Net: How Do They Learn To Protect Their Privacy? *Journal of Business and Economics Research* 2(9), 43-56.

MOWDAY RT and SUTTON RI (1993) Organizational Behavior: Linking Individuals and Groups to Organizational Contexts. *Annual Reviews in Psychology* 44 (1), 195-229.

ORVISKA M and HUDSON J (2009) Dividing or uniting Europe? Internet usage in the EU. *Information Economics and Policy* 21 (4), 279-290.

OYSERMAN D, COON HM and KEMMELMEIR M (2002) Rethinking individualism and collectivism: Evaluation of theoretical assumptions and meta-analyses. *Psychological Bulletin* 128(1), 3-72.

PALFREY J and GASSER U (2008) *Born Digital: Understanding the First Generation of Digital Natives*. Basic Books, New York.

PANOPOULOU E, TAMBOURIS E, ZOTOU M and TARABANIS K (2009) Evaluating eParticipation sophistication of regional authorities websites; the case of Greece and Spain. *Computer Science* 5694, 67-77.

PATTERSON P, COWLEY E and PRASONGSUKARN K (2006) Service failure recovery: the moderating impact of individual-level cultural value orientation on perceptions of justice. *International Journal of Research in Marketing* 23 (3), 263–277

PATTON MQ (1991) *Qualitative evaluation methods* (2nd ed.). Sage, New bury Park, CA.

PAVLOU PA (2011) State of the information privacy literature: where are we now and where should we go? *MIS Quarterly* 35 (4), 977-988.

PETTIGREW AM (1979) On Studying Organizational Cultures. *Administrative Science Quarterly* 24(4), 570-581.

PEIRCE CS (1931-1935). *Collected Papers of Charles Sanders Peirce*, 8 vols (HARTSHORNE C, WEISS P and BURKS AW, Eds), Harvard University Press, Cambridge, Massachusetts.

POLASIK M and WISNIEWSKI TP (2009) Empirical analysis of internet banking adoption in Poland. *International Journal of Bank Marketing* 27(1), 32-52.

POSEY C, LOWRY PB, ROBERTS TL and ELLIS TS (2010) Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities. *European Journal of Information Systems* 19, 181-195.

PRINCE M (1978) Focus groups can give marketers early clues on marketability of new product. *Marketing News* 12 (8), 12

REINERT M (1986) Classification descendante hiérarchique : un algorithme pour le traitement des tableaux logiques de grandes dimensions. In *Data analysis and Informatics* (DIDAY et al., Eds), pp 23-28, Elsevier Science Publishers.

REINERT M (1990). Alceste : une méthodologie d'analyse des données textuelles et une application : Aurélia de G. de Nerval. *Bulletin de Méthodologie Sociologique* 26, 24-54.

REINERT M (1998) *Quel objet pour une analyse statistique du discours ? Quelques réflexions à propos de la réponse Alceste*. In Proceedings of Journées Internationales d'Analyse Statistique de Données Textuelles (JADT), International Conference on textual data analysis, Nice, France.

ROUSSEAU D, SITKIN SB, BURT RS and CAMERER C (1998) Not so different after all: a cross-discipline view of trust. *Academy of Management Review* 23(3), 393-404.

RYAN AM, MCFARLAND L, BARON H and PAGE R (1999) An international look at selection practices: nation and culture as explanations for variability in practice. *Personnel Psychology* 52(2), 359–391.

SACKMANN SA (1992) Culture and Subcultures: An Analysis of Organizational Knowledge. *Administrative Science Quarterly* 37(1), 140-161.

SHENKAR O (2001) Cultural distance revisited: Towards a more rigorous conceptualization and measurement of cultural differences. *Journal of International Business Studies* 32 (3), 519-535.

SHIN SK, ISHMAN M and SANDERS GL (2007) An empirical investigation of socio-cultural factors of information sharing in China. *Information & Management* 44(2), 165-174.

SMITH HJ, DINEV T and XU H (2011) Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35 (4), 989-1015.

SMITH HJ, MILBERG SJ and BURKE SJ (1996a) Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly* 20 (2), 167-196.

SMITH PB, DUGAN S and TROMPENAARS F (1996b) National culture and the values of organizational employees: A dimensional analysis across 43 nations. *Journal of Cross-cultural Psychology* 27, 231-264.

SOLOVE DJ (2006) A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154 (3), 477-560.

SONDERGAARD M (1994) Research note: Hofstede's consequences: A study of reviews, citations and replications. *Organization Studies* 15, 447-456.

SRITE M and KARAHANNA E (2006) The role of espoused national cultural values in technology acceptance. *MIS Quarterly* 30 (3), 679-704.

STAAT W (1993) On Abduction, Deduction, Induction and the Categories. *Transactions of the Charles S. Peirce society* 29 (2), 225-237.

STEENKAMP J-B EM and GEYSKENS I (2006) How Country Characteristics Affect the Perceived Value of Web Sites? *Journal of Marketing* 70, 136-150.

STEEVES V and WEBSTER C (2008) Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society* 28(1), 4-19.

STRAUB D, LOCH K, EVARISTO R, KARAHANNA E and STRITE M (2002) Toward a Theory-Based Measurement of Culture. In *Human Factors in Information Systems* (SZEWCZAK EJ and SNODGRASS CR, Eds), 61-82, IRM Press, London.

TING-TOOMEY S (1991) Intimacy Expressions in Three Cultures: France, Japan, and the United States. *International Journal of Intercultural Relations* 15(1), 29-46.

TRIANDIS HC (1995) *Individualism and collectivism*. Boulder, CO: Westview Press.

TROMPENAARS F (1996) Resolving International Conflict: Culture and Business Strategy. *Business Strategy Review* 7(3), 51-68.

TUROW J and NIR L (2000) *The Internet and the family 2000: The view from parents, the view from kids*. Philadelphia, PA: Annenberg Public Policy Center, University of Pennsylvania.

VAN SLYKE C, SHIM JT, JOHNSON R and JIANG JJ (2006) Concerns for Information Privacy and Online Consumer Purchasing. *Journal of the Association for Information Systems* 7 (6), 415-444.

WANG YD and EMURIAN HH (2005) An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior* 21, 105–125.

WARREN SD and BRANDEIS LD (1890) The Right to Privacy. *Harvard Law Review* 4(5), 193.

WESTIN AF (1967) *Privacy and Freedom*. Atheneum Press, New York.

YOUN S (2005) Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media* 49(1), 86.

YOUN S (2009) Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs* 43(3), 389-418

Appendix 1. Justification for the countries chosen for the study (Eurostat 2008)

Block	Code	Country	1. ICT development			2. Socioeconomic development			3. Place in Europe		
			Percentage households with web access	Percentage households that use e-commerce	E-government availability and usage	GDP/capita in PPS	Employment growth	Youth education attainment	Date of entry into EU27	Geographical situation	Population (# inhabitants)
1	DK	Denmark	82	47	44	118.4	1.4	71.0	1973	NW	5475791
1	EE	Estonia	58	7	34	68.2	0.2	82.2	2004	NE	1340935
1	FI	Finland	72	33	53	115.1	1.6	86.2	1995	NE	5300484
1	LV	Latvia	53	10	16	55.8	0.8	80.0	2004	NE	2270894
1	LT	Lithuania	51	4	20	61.1	-0.5	89.1	2004	NE	3366357
1	SE	Sweden	84	38	52	121.5	0.9	87.9	1995	NE	9182927
2	BG	Bulgaria	25	1	8	40.2	3.3	83.7	2007	SE	7640238
2	CZ	Czech Rep.	46	13	14	80.1	1.2	91.6	2004	NE	10381130
2	HU	Hungary	48	8	25	62.8	-1.2	83.6	2004	SE	10045401
2	PL	Poland	48	12	16	57.6	3.8	91.3	2004	NE	38115641
2	RO	Romania	30	3	9	45.8	0.3	78.3	2007	SE	21528627
2	SK	Slovakia	58	13	30	71.9	2.8	90.2	2004	SE	5400998
2	SI	Slovenia	59	12	31	90.7	2.8	92.3	2004	SE	2010269
3	AT	Austria	69	28	39	123.1	1.8	84.5	1995	SE	8318592
3	BE	Belgium	64	-	16	113.9	1.9	82.2	1952	NW	10666866
3	FR	France	62	28	43	107.4	0.5	83.4	1952	SW	63982881
3	DE	Germany	75	42	33	116.1	1.4	74.1	1952	NW	82217837
3	IE	Ireland	63	30	27	136.6	-1.1	87.7	1973	NW	4401335
3	LU	Luxembourg	80	36	48	271.4	4.7	72.8	1952	NW	483799
3	NL	Netherlands	86	43	54	135.0	1.4	76.2	1952	NW	16405399
3	UK	UK	71	49	32	117.2	0.1	78.2	1973	NW	61193524
4	CY	Cyprus	43	7	16	94.7	2.6	85.1	2004	SE	789269
4	EL	Greece	31	6	10	93.9	0.1	82.1	1981	SE	11213785
4	IT	Italy	47	7	15	100.5	0.3	76.5	1952	SE	59619290
4	MT	Malta	59	16	20	75.5	2.5	53.0	2004	SE	410290
4	PT	Portugal	46	6	18	75.4	0.4	54.3	1986	SW	10617575
4	ES	Spain	51	13	29	103.4	-0.6	60.0	1986	SW	45283259

Appendix 2. Sample characteristics

Characteristics of the sample		Focus Group Sample*	
		Frequency	Percentage
Country	Estonia	19	13.7%
	France	20	14.4%
	Germany	21	15.1%
	Greece	20	14.4%
	Poland	20	14.4%
	Romania	20	14.4%
	Spain	19	13.7%
Gender	Male	65	46.8%
	Female	74	53.2%
Age	15-18	21	15.1 %
	19-24	44	31.7 %
	25-44	46	33.1 %
	45-60	18	12.9 %
	61 and more	10	7.2 %
Use of the Internet	1-3 years	14	10.1%
	3-5 years	24	17.2%
	+5 years	101	72.7%
Check emails	Several times per day	62	45.9%
	Once a day	38	28.1%
	Several times a week	27	20.0%
	Less than once a week	8	5.9%
Level of privacy concerns	Unconcerned	18	13.2%
	Moderately concerned	29	21.4%
	Very concerned	90	65.4%
Use of a pseudo	Never	87	62.6 %
	Yes/ Very often / Sometimes	43	30.9 %
Professional status	Still at school	19	13.7%
	Student	45	32.4%
	Salaried	28	20.1%
	Civil servant	15	10.8%
	Independent	10	7.2%
	Housewife or unemployed	13	9.3%
	Retired	8	5.8%
Marital status	Live with a partner	53	38.3%
	Live alone	35	25.2%
	Live at parents' home	51	36.7%
Education level	A level	36	26.5%
	Bachelor	70	51.5%
	Master	16	11.8%
	PhD	14	10.2%

*A total of less than 139, or 100 percent, occurs because some people did not answer all questions.

Appendix 3. Process of data collection and analysis

STEP 1. DATA COLLECTION

- Two focus groups organized per country (one with young people and one with adults), 7 countries (14 focus groups), a total of 139 participants (8 to 12 in each focus group)
- All moderators are scholars of partner universities, having a very good knowledge of English
- The same instructions are given to the partners to recruit participants
- Before the beginning of each focus group, participants completed a questionnaire to indicate their individual characteristics (see Appendix 2)
- The same guide was used by all moderators, trained and briefed in advance
- The moderator and participants use their common native language during the discussion
- The same moderator conducts the two focus groups in his or her country
- All the discussions are audio and video-recorded
- Each moderator is in charge of the transcription of the focus groups he or she conducted
- Each moderator is in charge of the translation of the discussions in English
- All the discussions translated into English are sent by the moderators to the authors

STEP 2. PREPARATION OF THE CORPUS BY THE RESEARCHERS

A global corpus of all translations of the discussions in the 7 countries is prepared for the analysis: a partition of the corpus is made to separate the discourse of each of the 139 participants. Thus, each sentence pronounced by one participant can be linked to the number of the participant, to the country, to one of the two focus groups of the country, and to the individual characteristics of this participant. With Alceste software, the separation is a row beginning with the number of the participant (4 characters) and then the character "*". The individual characteristics are added after the "*".

> Example:
> 0001 *Country_Estonia *Gender_F *Age_19to24 *FG_Young
> Text of the focus group participant number 1, an Estonian female, aged between 19 and 24, interviewed in the focus group with young people
>
> In this file, participants 1 to 19 are from Estonia; participants 20 to 39 are from France; participants 40 to 59 are from Romania; participants 60 to 80 are from Germany; participants 81 to 100 are from Greece; participants 101 to 120 are from Poland; participants 121 to 139 are from Spain.

Seven files (one per country) are also prepared in the same way to run detailed analyses per country.

STEP 3. DATA ANALYSES BY THE SOFTWARE PACKAGES

ALCESTE SOFTWARE

- Segmentation of the corpus and reduction of the words to their roots (lemmatisation): The software identifies the set of lexicometrical base units in the corpus. Each unit is named a graphical form, or word-type (Lebart & Salem, 1994). The software identifies more complex forms and thus regroups into units the graphical forms that correspond to the different ways in which the same lemma can occur (e.g., verbs changed to infinitives, plurals to singular). In the standard analysis, rare words (frequency less than 4) are eliminated.

- Partition of the corpus by the software: The Alceste software divides the text into contextual units (CUs) that correspond more or less to a small paragraph, depending on the length of the corpus. The entire corpus is separated into different CUs. The lexical table cross-tabulate the lemmatized forms, with the text separated into different contextual units (CUs). The rows of the data table correspond to the different CUs, and the columns correspond to the different graphical forms (lemmatized words). The cells contain either 0 or 1 (complete disjunctive table), depending on the absence or presence, respectively, of the graphical form in a CU.

Example:

	Lemmatised word 1	Lemmatised word 2	Lemmatised word 3	Lemmatised word 4	…
CU number 1	0	1	1	1	…
CU Number 2	1	1	0	0	…
…	…	…	…	…	…

- Descending Hierarchical Classification (DHC)

A DHC is performed on the entire lexical table. A second classification tests the stability of the classes obtained. In this second classification, each CU is longer (minimum of 12 words instead of 10 in the standard configuration). In the classification, all the CUs are first placed together in a single class. Then, at each step, the two most different classes (i.e., with the greatest margin contrast) are identified until all CUs have been either classified or not, depending on their graphical forms.

WORDMAPPER SOFTWARE

- Segmentation of the corpus, identification of "significant words" (meaningful) and reduction of the words to their roots (lemmatisation): any WordMapper analysis must begin with the creation of meaningful words, and during that phase, empty words, such as articles, are eliminated. In the standard analysis, rare words (frequency of the word in the corpus less than 3) and non-significant (empty) words (number of letters less than 3) are eliminated. The software establishes the list of all the significant words with a minimum frequency of 3.

- Construction of the data table by the software: the list of the lemmatised significant words is used by the software to build the data table. The rows of the data table correspond to the different lemmatised significant words, and the columns correspond to the different modalities of the variable chosen.

Example for the variable "country":

	Country Estonia	Country France	…
Lemmatised significant word 1	Frequency of word 1 in the Estonian participants discourses	Frequency of word 1 in the French participants discourses	…
Lemmatised significant word 2	Frequency of word 2 in the Estonian participants discourses	Frequency of word 2 in the French participants discourses	…
…	…	…	…

- A correspondence factor analysis (CFA) is performed on the data table.

STEP 4. INTERPRETATION OF THE RESULTS BY THE RESEARCHERS

RESULTS WITH ALCESTE SOFTWARE

A dendogram resulting from the DHC shows the hierarchical division of the classes (each class, i.e. a group of co-occurring words, forms a specific lexical world). In practice, what is important is the stability of the classes obtained, and the percentage of CUs globally classified. The individual characteristics of the participants are not taken into account when classifying the responses (they are supplementary elements), but it is possible to describe each class in terms of its population. The software calculates the representativeness of each word and each CU for a specific class, according to the chi-square statistic (see Appendix 4).

RESULTS WITH WORDMAPPER SOFTWARE

The statistics given by the software help the researcher to interpret the results of the CFA. These statistics are the same and the interpretation is the same as a CFA performed on non-textual data: absolute contributions per axis, relative contributions (squared cosine) per axis, coordinates per axes.

Appendix 4. Example calculation of chi-square with Alceste

	Form J present	Form J absent	
Class C	25 (4)	5 (26)	30
Complementary to Class C	15 (36)	255 (234)	270
Text	40	260	300

Notes: In this example, 25 is the real frequency of the graphical form J (lemmatised word) in class C, and (4) is the theoretical frequency (if J is equally present in the different parts of the corpus). Chi-square = $[(25 - 4)^2/4] + [(5 - 26)^2/26] + [(15 - 36)^2/36] + [(255 - 234)^2/234] = 141.34$. All the chi-squares calculated by Alceste are based on a table with two rows and two columns (margins not taken into account), so the degree of freedom [(number of rows – 1) × (number of columns – 1)] always equals 1. Thus, all chi-squares greater than 10.8 correspond to the graphical forms 'representative' or 'specific' with a probability < 0.001. Here, we can say that the J form is highly specific to class C.

Appendix 5. Examples of interactions during the focus groups

Focus group with young people, France, Discussion about 'Responsibility'

Participant number 22

If you trust a website you also don't want that Internet site or company to give out your information either. So the responsibility for the site is not just ours.

Participant number 24

At the same time if there's a problem you're not going to go and complain to the site.

Participant number 22

It's a bit pointless... you can only blame yourself.

Participant number 23

Yes because you don't know if behind it there's actually a person at all. So you're not going to get angry... well yeah you get angry with the computer at the time, but the computer is not going to give you an answer. So then you blame yourself. The problem is when you get a call from a call centre, you don't know how to take your information back. If they start rattling off the details of your life you're not going to say: "no that's not me".

Participant number 20

Your reflex is to hang up, but a better thing to do would be to ask them how they got your information.

Participant number 23

At the same time they use formulaic questions and you just answer them.

Participant number 24

Then you can tell them for your landline you don't want to or you don't agree with that kind of technique.

Focus group with young people, Greece, Discussion about 'Trust'

Moderator

How can companies gain your trust, so that you will give them your data?

Participant number 87

Mainly by being well-known.

Participant number 88

I gave it to a company, only because a friend of mine was working there.

Participant number 90

To be trustworthy actually. Not just having a good reputation, the company must also have terms of use, and we must be certain that the data will not be used for another purpose.

Participant number 81

…If I were asked something irrelevant, I would be suspicious, why is he asking me that? I would question its motives, when I can't imagine how the company will use it.