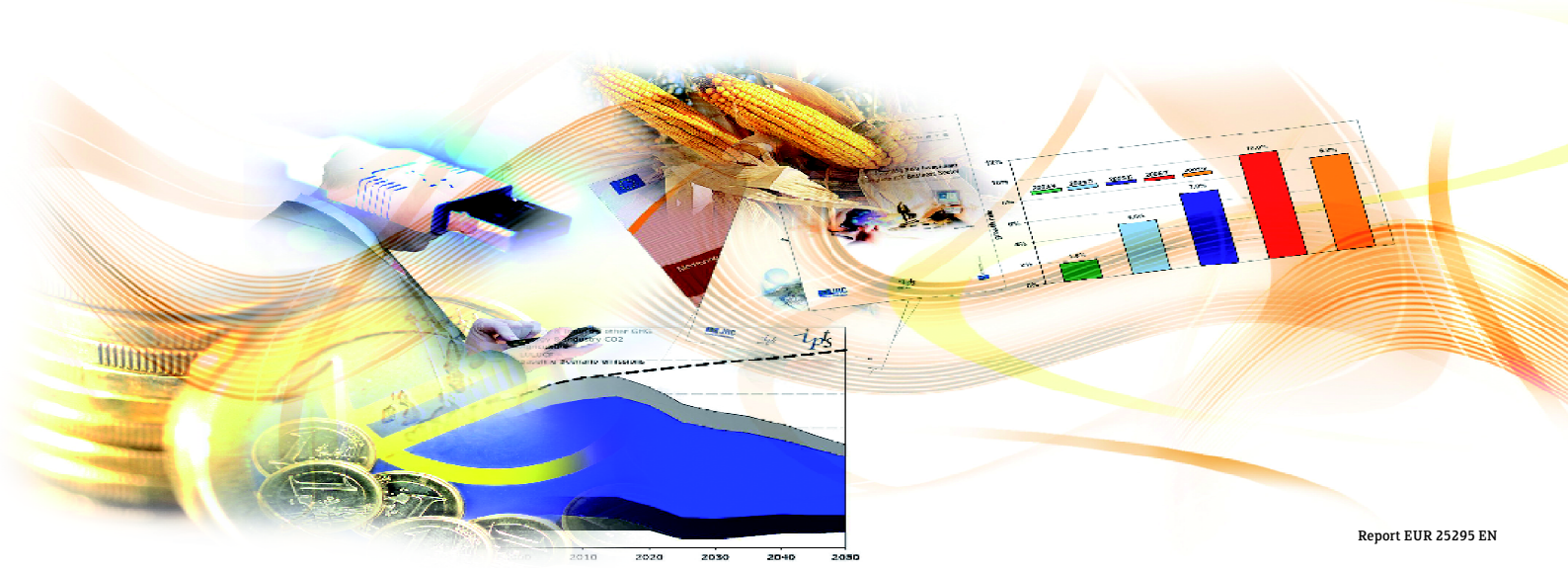
European Commission

JRC SCIENTIFIC AND POLICY REPORTS

Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management

Authors
Wainer Lusoli, Margherita Bacigalupo,
Francisco Lupiañez, Norberto Andrade,
Shara Monteleone, Ioannis Maghiros

2012



Report EUR 25295 EN

Joint Research Centre

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information
Address: Edificio Expo. c/ Inca Garcilaso, 3. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300

http://ipts.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

This publication is a Reference Report by the Joint Research Centre of the European Commission.

JRC 70301

EUR 25295 EN

ISBN 978-92-79-23914-4

ISSN 1831-9424

doi:10.2791/81962

Luxembourg: Publications Office of the European Union, 2012
Rome: Food an Agriculture Organization of the United Nations

Printed in Spain

Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management

Authors:
Wainer Lusoli, Margherita Bacigalupo, Francisco Lupiañez, Norberto Andrade, Shara Monteleone, Ioannis Maghiros

2012

EUR 25295 EN

Acknowledgments

After three years of work, the list of people we feel deserve our gratitude grows considerably long.

We would like to start this long list by highlighting our appreciation to Caroline Miltgen (GRANEM, University of Angers) and Christine Balagué (University of Lille) who contributed to the inception phase of the survey. Also, we are grateful to the members of our Scientific Committee and to the participants to the survey expert workshop, who commented and validated preliminary results and helped us brainstorm a number of thorny issues. This list is long and we mean no offence by mentioning them by their first name, namely:

Ellen Helsper, London School of Economics; Marc van Lieshout, TNO; Carlos Flavian, Universidad de Zaragoza; Thierry Nabeth, INSEAD; Neil Robinson, RAND Europe; Ingo Naumann, ENISA; Jean-Marc Dinant, CRID (Centre de recherche informatique et droit); Masashi Ueda, National Institute of Informatics, Japan; Ayako Komatsu, ISEC, IPA, Japan; Laurent Beslay, European Data Protection Supervisor (EDPS}; Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada; Caspar Bowden, Microsoft; Alain Heureux, IAB Europe; Fran Meier, TrustE; Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein, Germany; Reinhard Posch, CIO Federal Government Austria;

We wish to thank our colleagues at DG INFSO for a working relation that that went far beyond contractual obligations, professional duty and inter-institutional good will. In them, we always found intelligent, critical readers, informed and committed professional. Among others who gave their time, we are very grateful to Michal Hrbaty, who kept a very close eye on the project from the beginning to almost the very end; to Anne Troye and Beatrice Covassi who saw it begin in 2008, and to Ken Ducatel, Frank Boissiere and Kristiina Pietikainen for their involvement in taking it to fruition.

We also wish to thank colleagues at DG Justice, as their assistance made possible to field a much richer survey than would have been possible otherwise. Our gratitude also extends to DG COMM, a Commission service without which the Eurobarometer would not have been an option for us. Also to TNS Opinion, which collected quality data across EU27 and compiled the special Eurobarometer report.

At JRC IPTS, we are grateful to Ramon Compañó. Had he not, in the meanwhile, taken up a new position as IPTS Director's Assistant, he would have co-authored this report in his usual style, and perfectionist attitude. Last but certainly not least we would like to thank David Broster, our Head of Unit, who steered this work from the beginning and provided his invaluable advice during the critical stages of the development.

The eID team at the Institute for Prospective Technological Studies (IPTS) of the Joint Research Centre (JRC) managed the design, analysis and interpretation of Special Eurobarometer 359 on Electronic Identity and Data Protection. DG Justice contributed to the finalization of survey questions in relation to data protection. TNS Opinion conducted the survey in EU27 and contributed to preliminary data analysis.

The interested reader will find all documents[1] related to the project on the JRC IS Unit website, at: http://is.jrc.ec.europa.eu/pages/TFS/dl.html. For further queries, please contact Ioannis Maghiros [ioannis.maghiros@ec.europa.eu].

1 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Table of Contents

List of Figures

List of Tables

Preface

We live in the age of disclosure: personal data circulates relatively freely across borders, and citizens are able to create and control multiple identities. Personal data underpins most digital services: search, social networking, eCommerce, eHealth. Personal data also enable businesses to provide new, intelligent and automated services to their customers. But not all is rose-tinted in the digital world.

The present survey provides new evidence that European citizens favour strong and secure privacy, identity and data protection rights. Europeans care a lot about their personal information, about their privacy and about their digital identity. Although the perception of our identity as well as that of others has always been important, the advent of the Internet has increased the importance of personal information, since online identity is what allows us to share information and access data, services and applications. Personal data is today indispensable to live our digital lives.

The survey suggests that our use of, and dependence on, the Internet, mobiles and other devices has highlighted the need to regulate and better control the identification process in a global digital world. There is big demand for secure and interoperable e-authentication tools that can reduce our vulnerability towards misuse and abuse of personal data such as identity theft, personal data loss and profiling.

2011 was a year of review, both in Europe and more broadly. I hope that many will find therefore fresh evidence in what follows for improved behaviour, stronger policy and better business models.

Robert Madelin
Director General
Directorate General Information Society and Media

Executive Summary

This Report presents the results of the largest survey ever conducted in Europe and elsewhere about people's behaviours, attitudes and regulatory preferences concerning data protection, privacy and electronic identity, both on the Internet and otherwise in their daily lives. It finds that personal data disclosure is increasingly prevalent in the European society, largely due to the expansion of the Information Society. In turn, most services provided in the digital economy rest on the assumption that this data and associated electronic identities are collected, used and disposed of according to existing legislation.

The survey shows very clearly how Digital Europe is shaping up. About two thirds of EU27 citizens use the Internet frequently, more than one third uses Social Networking Sites (SNS) to keep in touch with friends and business partners and almost 4 out of 10 shop online. In both of these contexts, people disclose vast amounts of personal information, and also manage a large and growing number of electronic identities. However, there are equally significant differences among Member States and considerable digital exclusion, mainly due to socio-demographic differences in affluence, education and age.

Europeans know that if they want to benefit from using the Internet to its full potential they have to disclose their data (biographical, social, financial or medical) and manage online identities. Almost three in four Europeans accept that revealing personal data, so as to benefit from online services, is part of everyday life. While nearly all disclose biographical data (i.e. name, nationality, online account identity) to access a service, users shopping online also disclose address information and financial information and users of social networking sites disclose more social information but not financial.

But online users are also very much aware of risks in transacting online and are naturally concerned. The perception of risk is greater for more 'mature/active' users but it does not seem to curb abuse and misuse – such as data loss and identity theft. Providentially, these are still uncommon in Europe. Furthermore, Europeans understand they are not in control – an impressive 30% of all eCommerce users that disclose information believe they have no control on their data. They employ a variety of methods, both in the offline and the online world, to protect their identity; however, they tend to understand better how to protect their identity in the offline world (62% use data minimisation techniques) than when in the online world (about 40% use anti-spam and anti-spy software). Finally, almost all Europeans (90%) favour equal protection of their data protection rights across the EU, even though a majority feel responsible themselves for the safe handling of their personal data.

Finally, people trust institutions more than companies, especially medical institutions, to protect the data they are entrusted with; they are slightly less sanguine about whether Governments and Banks are to be trusted and concur as to the perception that private companies such as Internet service providers, e-shops and telephone companies are not to be trusted with their data.

These are some of the insights of the Eurobarometer survey[2] on Data Protection and Electronic Identity which was conducted in December 2010 and the results of which were released[3] and published[4] in June 2011.

The present report[5] builds on the top line results presented in the EB-359 report and analyses in depth the information collected so as to draw conclusions in direct relation to four Digital Agenda key areas: e-Commerce, Social Networking sites, Authentication and Identification and Medical information as personal data.

More in detail, this report finds:

1 As eCommerce is becoming mainstream in Europe (about 40% of EU27 citizens engage in this activity), the fact that virtually nobody shops cross-border in-EU or out-EU without shopping first in their own country points at the need to promote cross-border eCommerce by enforcing legislation to enhance 'trust' within national borders first. Reinforcing trust of young people is particularly important, as the younger generation harnesses the Internet in more depth.

2 With socio-demographics (i.e. affluence, education, age) underpinning Internet uptake and an almost perfect correlation between Internet use and eCommerce, both factors strongly influence online shopping; they are at least as important, if not more, than national factors such as regulation, supply of services or structure of the digital market.

3 There is significant use of business-issued rather than public-issued credentials for all Internet transactions, especially for eCommerce; in part, this depends on the fact that although many countries issue credentials these are seldom directly usable online for commercial purposes. This implies that:

   a) A transaction system based on the use of third-party credentials, rather than on direct disclosure of bank or credit related information, and in general other ways of pegging 'virtual identity' to real identity may enhance accountability and be useful to stimulate cross-border shopping.

   b) The offer of interoperable, easy to use national and cross-border systems with similar look and feel and more uniform protection of the rights of consumer and their personal data across the EU contribute to making it easier to transact cross-border.

4 With small differences in socio-economic traits and country of residence, people consider themselves and companies as being responsible for the protection of their data, rather than policymakers [of course, each in their own capacity]. Explicitly better enforcement of existing Data Protection rules accompanied by an increase of awareness of rights is seen as required. Implicitly, this suggests that fostering [genuine] trust in data controllers and their practices may remove part of the burden from regulators' shoulders.

2 The eID team at the Institute for Prospective Technological Studies (IPTS) of the Joint Research Centre (JRC) and DG Justice managed the design, analysis and interpretation of Special Eurobarometer 359 on Data Protection and Electronic Identity. TNS Opinion conducted the survey in EU27 and contributed to data analysis. The survey was coordinated by the DG COMM "Research and Speechwriting" Unit.

3 See: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/742&format=HTML&aged=0&language=EN&guiLanguage=en

4 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

5 Deliverable D3 of the AA 31508-2009-10 between DG INFSO/C1 and JRC-IPTS on analysis of results.

5 The perception of risk associated with eCommerce and Social Networking is not acknowledged as a dominant factor. The more people carry out Internet activities the more likely they are to shop across borders, even though the perception of risk increases. An explanation may come from the finding that people who fear risks are also more likely to take active steps to protect their personal identity, both offline and online.

6 More needs to be done to raise awareness regarding the identity-related personal data users regularly provide online; differences in the use of identification data are unrelated to macro-economic indicators but they mirror the structure in place in single countries. If cross-border eGovernment or eCommerce are to be fostered, then a more homogeneous use of government-related identification data would be needed.

7 People who use government-issued credentials are both more likely to report reduced perception of risk of identity-theft and to trust companies less as data controllers. In turn, people who trust companies less are less likely to engage in a range of Internet activities, including eCommerce. Therefore, some degree of 'portability of trust' from public to commercial institutions could be fostered via the greater use of government-supported, if not outright issued, credentials.

8 The media play a vital role in generating support for more articulated awareness of the challenge of identity or data loss. Since Internet users are largely sensitive to the media, these may be used to 'nudge' Europeans in the direction of improved protection of their identity-related data with online protection tools or by minimising personal data disclosure. The latter is particularly important in the case of the 'significant' minority of Europeans who are very open to disclose personal data, trust companies and are comfortable with online profiling and practically do not use measures to protect their data. From another point of view 'nudging' could be facilitated if accompanied by stricter rules to prevent abuse.

9 Independent of whether people use private- or public- issued identification data they are strongly in favour of the key principles of the existing European Data Protection legislation: (i) homogeneous data protection rights across the EU; (ii) to be informed when their personal data is lost or stolen; (iii) to be able to delete/edit their data whenever they wish to do so. This is a loud and clear call for stronger enactment, in everyday life, of these principles. This may also indicate a trend towards more institution-centred remedies (i.e. on regulating directly the controllers, processors of information) rather than more personal initiative (i.e. burdening the data subjects with necessary proactive online strategies for the protection of their identity online).

10 Overall, results suggest that public institutions have large room for manoeuvre in addressing problems of trust and safe use of credentials in online transactions – today the role of public credentials is largely marginal to the structure of eServices in most EU countries. It emerges clearly that Member States need to coordinate their respective eID actions, if the potential of credentials is to enable an increase in the fruition of eServices both public and commercial; especially, this is the case in MS with a less established culture of credentials, lower levels of eCommerce and lesser Internet skills.

11 More than a third of EU27 (34%) access Social Networking Sites (SNS), and more than half of those also use websites to share pictures, videos, movies, etc… The main use of SNS is to enable online socialising which necessarily means disclosing of social (personal) information online; indeed SNS users are less cautious about sharing social information although they consider it personal. There are

notable differences in the geographical use of SNS amongst Member States. There is also a generation split as younger people use the Internet very little outside SNS in all MS while older people who use SNS are practically the same as a percentage of Internet users.

12 The last point is important, as the younger generation (Digital natives) tends to behave in a significantly different fashion from their parents; results suggest that this may go beyond lifecycle effects, as not-so-young adults also disclose more, control less and are equally worried about their privacy. Thus the policies and regulatory framework of today may need overhauling in the next 10-20 years. In the interim, policy initiatives need to provide support for the commercial 'nudging' of the relatively younger generation (40-55 years of age) to behave responsibly with their data.

13 Significant work will be needed to enforce fully informed consent and to foster better awareness of what may happen with people's personal data once it is disclosed in an SNS. Such initiatives would need to address both: (i) what SNS ought to do to inform their users on how data collected will be used and what the consequences of such use may be; and (ii) what SNS users may demand as just return to their consent towards their personal information being used to extract monetary value from (i.e. behavioural advertising).

14 This is especially so in the case of those Europeans (3-5%), who albeit consider their medical data to be personal, do disclose it. Since they are aware of the risks that this may involve, one may deduce that the benefit from disclosure is high enough. In this case significant protection may be needed; especially since currently the controllers of such information are private companies who are less trusted online. The latter may indicate an opportunity for 'trusted' public services to become available.

15 Finally, the survey indicates strong support for a number of technical solutions to challenges, such as the need for systems that: (i) allow portability of trust from public to commercial institutions via the greater use of government-supported, if not outright issued, credentials; (ii) a disclosure system based on third-party credentials, and other ways of pegging 'virtual identity' to real identity; and (iii) interoperable, easy to use national and cross-border systems with similar looks and feel.

1 Study Design and Survey Methodology

1.1 Survey methodology

The survey was conducted by TNS in the 27 Member States of the EU between the 25 November and 17 December 2010. 26,574 Europeans aged 15 and over, resident in each EU Member States (MS), were interviewed. The full breakdown of interviews by Member States and relevant data collection dates are reported in Table 1. The methodology used is that of the Standard Eurobarometer. In short, the survey design applied in all MS is a multi-stage, random probability sample.

More in detail, in each country, a number of sampling points was drawn with probability proportional to population size (for a total coverage of the country) and to population density. In order to do so, the sampling points were drawn systematically from each "administrative regional units", after stratification by individual unit and type of area. They thus represent the whole territory of the countries surveyed according to the EUROSTAT NUTS II (or equivalent) and according to the distribution of the resident population of the respective nationalities in terms of metropolitan, urban and rural areas. In each

Table 1. Survey schedule by country

Abbreviations	Country	# interviews	Fieldwork started	Fieldwork ended	Population 15+
BE	Belgium	1020	25/11/2010	14/12/2010	8,866,411
BG	Bulgaria	1000	26/11/2010	08/12/2010	6,584,957
CZ	Czech Rep.	1015	26/11/2010	13/12/2010	8,987,535
DK	Denmark	1007	26/11/2010	15/12/2010	4,533,420
DE	Germany	1519	25/11/2010	12/12/2010	64,545,601
EE	Estonia	1000	26/11/2010	13/12/2010	916,000
IE	Ireland	975	26/11/2010	17/12/2010	3,375,399
EL	Greece	1000	26/11/2010	13/12/2010	8,693,566
ES	Spain	1006	26/11/2010	14/12/2010	39,035,867
FR	France	1000	26/11/2010	14/12/2010	47,620,942
IT	Italy	1039	26/11/2010	13/12/2010	51,252,247
CY	Rep. of Cyprus	501	26/11/2010	12/12/2010	651,400
LV	Latvia	1000	26/11/2010	13/12/2010	1,448,719
LT	Lithuania	1026	26/11/2010	13/12/2010	2,849,359
LU	Luxembourg	501	26/11/2010	15/12/2010	404,907
HU	Hungary	1014	26/11/2010	13/12/2010	8,320,614
MT	Malta	500	26/11/2010	12/12/2010	335,476
NL	The Netherlands	1024	26/11/2010	14/12/2010	13,288,200
AT	Austria	1010	26/11/2010	12/12/2010	6,973,277
PL	Poland	1000	26/11/2010	13/12/2010	32,306,436
PT	Portugal	1046	26/11/2010	13/12/2010	8,080,915
RO	Romania	1013	26/11/2010	10/12/2010	18,246,731
SI	Slovenia	1020	26/11/2010	13/12/2010	1,748,308
SK	Slovakia	1034	26/11/2010	13/12/2010	4,549,954
FI	Finland	1003	26/11/2010	16/12/2010	4,412,321
SE	Sweden	1010	26/11/2010	15/12/2010	7,723,931
UK	United Kingdom	1291	26/11/2010	14/12/2010	51,081,866
Total EU27		26,574	25/11/2010	17/12/2010	406,834,359

of the selected sampling points, a starting address was drawn, at random. Further addresses (every Nth address) were selected by standard "random route" procedures, from the initial address. In each household, the respondent was drawn, at random (following the "closest birthday rule"). All interviews were conducted face-to-face in people's homes and in the appropriate national language. As far as the data capture is concerned, Computer Assisted Personal Interview (CAPI) was used in those countries where this technique was available.

1.2 Study design

Overall, survey design is based on the concept and practice of personal data disclosure in context; it takes the move for the assumption that personal data disclosure is prevalent, to some extent unavoidable, in modern European and non European societies. It looks at Online Social Networking and eCommerce as two principle contexts where disclosure ifs particularly policy sensitive. In the process, it examines issues of privacy, data protection and identity. Specifically, authentication and electronic identities are examined as a possible mitigation to the prevalence of disclosure across contexts. The survey includes 47 questions on these topics, alongside usual questions on respondents' socio-demographic profile. The full questionnaire is provided in Annex: Survey Questionnaire.

Due to its complex nature, the survey was a long time in the making, a journey starting in 2008 and now completed upon publication. Quality checks and scientific validations along this time ensure that the survey actually measures what it aims to. Several preparatory activities, described below, lead up to survey execution.

- Desk research [2007-2010]
  - Exhaustive review of literature and current research on themes of data protection, identity management technologies and practices, digital identity, privacy, user online behaviour, online social networking and eCommerce, regulation and self-regulation. Review of policy developments in data protection, eCommerce, privacy, e-signature and authentication, electronic identity.

- 2 sets of focus groups with young people [January-February 2008]
  - Two discussion groups of eight to 12 people aged 15-25 years were held during January and February 2008 in Spain, France, Germany and Britain.

- Validation workshop [April 2008]
  - Involved 16 external experts from various disciplines cognate with survey topics. Here, the aims of the pilot survey were discussed, to improve both the theoretical framework and the data collection methodology.

- Survey pilot in 4 countries [UK, Spain, France and Germany], conducted using scenarios with people aged up to 25 years of age, online [July-August 2008].

- Focus groups with people of all ages and young people, in 7 countries, on themes concerning the definition and disclosure of personal data, and notions of privacy and control [February 2010]
  - Seven European countries representative of regional areas. Two discussion groups in each country, with eight to 12 participants each and with 139 participants in total.

- Validation workshop [April 2010]
  - Involved 10 external experts from various disciplines cognate with survey methodology and design. Here, the scientific framework of the survey was discussed, to arrive at the final questionnaire.

- Survey finalization [May-November 2010]

1.3 Analysis and reporting

Unless otherwise specified, percentages reported in the Report are based on weighted data, nationally and at EU27 level. This means that responses are weighted within countries to make them representatives of actual social distribution, and of the actual size of different countries in terms of population, so as to represent faithfully Europe's views. For each country a comparison between the sample and the reality was carried out. This 'reality check' was based on data on the actual composition of the population from Eurostat and/or from national statistics offices. For all countries, a national weighting procedure for gender, age, region and size of locality, using marginal and intercellular weighting, was carried out based on this fuller picture. For international weighting (i.e. EU averages), official population figures as provided by EUROSTAT or national statistic offices were used. When national results are reported, results are based on national weighted data only (the first described above). When results are reported for Europe, both sets of weights are used.

Figures and percentages are rounded at the lowest significant value, to the nearest integer (e.g., 1% rather than 1.2%, and 2% rather than 1.6%). For some questions, ones that allowed multiple responses, percentages necessarily add up to more than 100%. This are clearly marked in table footnotes. Statistical measures of significance are also reported in some tables and across the text, using the standard 'p value'. Statistical significance indicates the extent to which results may be due to chance, as only a sample of EU citizens were interviewed and not all. Traditionally for large samples, only results where this chance is below 5% are considered valid.

Across the various sections of the Report, two data analysis techniques, namely factor analysis and multi-dimensional scaling, were used jointly to help determine the structure of data and to reduce their complexity. Factor analysis is a technique that aims at reducing the complexity of data. It does so by creating clusters (so-called dimension) of similar variables based on what people actually respond to each of them. If people responds consistently 'yes' or 'very much' to different (but related) questions, we assume that an underlying behaviour can be identified. If this is the case, factor analysis helps extract 'dimensions' and build scales (e.g. 1 to 10) on the basis of these dimensions. Dimensional scales are then used in further analysis, in relation to other variables and other dimensions (if any exist, of course). There is debate in the scientific literature on whether one can create reliable scales out of factor analysis of dichotomous items (e.g. yes/no questions), as these items lack the depth of information required by the technique. Therefore we checked the results with a technique known as multi-dimensional scaling. This technique measures the distance between responses in a way that better respects the yes/no nature of the data. However, as a note of caution, this technique does not allow the use of national and EU27 weights.

2 FACT SHEET: eCommerce

2.1 Question context

The questionnaire included several questions regarding disclosure and protection of personal data disclosed in the context of eCommerce, see Table 2:

Table 2. eID survey questions relevant to eCommerce

Question code	Shorthand	Formulation	Rationale
QB4b	Personal data disclosure	Thinking of the occasions when you have purchased goods or services via the Internet, which of the following types of information have you already disclosed?	To gauge the extent of disclosure of different types of personal data; this question follows on a previous questions asked of all respondents regarding what information they though was personal.
QB5b	Reasons why disclose	What are the most important reasons why you disclose such information in online shopping?	To asses the reasons why people disclose personal data in eCommerce, whether for leisure, to get better offers, to save time, etc.
QB6b	Control on information disclosed	How much control do you feel you have over the information you have disclosed when shopping online, e.g. the ability to change, delete or correct this information?	To determine the level of perceived control on the data disclosed in eCommerce. This is related both to the right of access to one's information, and to the capacity of people to actually control their data once they have disclosed it.
QB7b	Risks related to disclosure	I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of your personal information to buy goods or services via the Internet?	To explore the risks people associate with the disclosure of personal data in eCommerce. Several risks may be associated with disclosure, including risks to reputation, to personal safety, to data integrity and others.
QB8b1 & QB8b2	Responsibility to protect	Who do you think should make sure that your information is collected, stored and exchanged safely when you buy goods or services via the Internet? Firstly? And secondly?	To help determine who people think is responsible for the protection of personal data once it's been disclosed.

2.2 Legal context

The main legal instruments in the area of eCommerce are the following:

- Electronic Commerce Directive: Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce in the Internal Market. It creates the basic legal framework for electronic commerce in the Internal Market, removes obstacles to cross-border online services in the European Union and provides legal certainty to business and citizens alike. It also establishes harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers.

The low numbers of online purchases cross border, and the very little difference between percentages of people buying inside and outside the EU, underline the relative lack of success of the Directive in promoting "trust" in eCommerce sites located outside the Member State of the buyer, as well as in the digital single market as a whole. Moreover, it is seen as encouraging self-regulation and "privacy/identity by design" solutions.

- The Distance Selling Directive: Directive 97/7/EC on the protection of consumers in respect of distance contracts. This directive applies to any consumer distance contract made under the law of an EU-Member State as well as the European Economic Area (EEA). It provides a number of fundamental legal rights for consumers in order to ensure a high level of consumer protection throughout the EU.

- Additional EU-wide law includes: (the choice of) law applicable to contractual obligations (Rome Convention 1980); jurisdiction and enforcement of judgments (Brussels Regulations 44/2001); unfair terms in consumer contracts (93/13/EC); the sale of goods and associated guarantees (1999/44/EC); and e-money (2000/46/EC).

Other important directives and strategic documents within the eCommerce legal framework are the following:

- Data Protection Directive: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This directive is the general EU law in the field of protection of personal data and the most prominent legislative act regulating the processing of personal data. Its objective is to protect the privacy of individuals while enabling the free flow of personal data within the EU in the context of the internal market. It lays down obligations on data controllers and specifies the rights of data subjects.

The results presented in this fact sheet seem to indicate a societal change in the perception of privacy vis-à-vis the one entailed in the current EU legislation. This is based on the observed behaviour regarding the disclosure of personal information [what is considered personal data and what is disclosed]. In essence, although a large majority of people consider identifiers (such as name, address, nationality, financial information) as personal information, they are obliged to disclose it on eCommerce sites. Without doubt this behaviour is eroding the established values of privacy and identity as these are defined in the directive. eCommerce users' control over their own information in eCommerce sites is another issue that relates to the implementation of the Directive.

- ePrivacy Directive: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. This directive particularises and complements the Data Protection directive with respect to the processing of personal data in the electronic communications services over public communications networks to ensure confidentiality of communications and security of their networks, including an obligation to notify personal breaches to the competent authority at national level. This directive is relevant and applicable in the case of disclosure of personal information in the online environment, namely in eCommerce sites.

- Directive 98/48/EC of the European parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. This Directive provides the definition of information society services (Art.1(2)) which applies to eCommerce sites.

- Digital Agenda: The Communication named "A Digital Agenda for Europe." is one of the seven flagship initiatives of the Europe 2020 Strategy, set out to define the key policies and actions necessary to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable applications.

  The low numbers of eCommerce cross border transactions identified in this fact sheet is also confirmed by the DAE scoreboard: "*less than one in ten eCommerce transactions are cross-border*".

  The DAE key actions planned by the EC in the area of self-regulation and alternative dispute resolution (*EU-wide Online Dispute Resolution system for eCommerce transactions by 2012*) are confirmed by attitudes identified in relation to the allocation of responsibility for the protection of personal data to individuals and companies (rather than to public authorities)

  The strong correlation between Internet use and proportion of people shopping online (frequent users shop more across borders) emphasizes the relevance and urgency of Key Action 8: "[a]dopt in 2010 a Broadband Communication that lays out a common framework for actions at EU and Member State to meet the Europe 2020 broadband[6] targets."

2.3 Location of eCommerce: national, x-border and out-EU[7]

European Internet users were asked what activities they undertook online [Table 3]. A majority of Internet users (60%) reported purchasing goods or services online, such as travel, holiday, clothes, books, tickets, film, music, software, or food. eCommerce is becoming mainstream in Europe as about 40% of all citizens engage in this activity.

Table 3. Purchase of good and services online at different locations

	% of Internet users	% of EU 27 population
Purchase goods or services online/ online shopping	60%	39%
Buy goods in own country	46%	30%
Buy goods in EU	18%	12%
Buy goods outside EU	13%	8%

Base: Internet users and EU27.

Source: QB1a & QB1b.

6 The Europe 2020 Strategy has underlined the importance of broadband deployment to promote social inclusion and competitiveness in the EU. It restated the objective to bring basic broadband to all Europeans by 2013 and seeks to ensure that, by 2020, (i) all Europeans have access to much higher internet speeds of above 30 Mbps and (ii) 50% or more of European households subscribe to internet connections above 100 Mbps.

7 QB1a For each of the following activities, please tell me if it is an activity that you do, or not, on the Internet. 3. Purchase goods or services online\ online shopping (e.g. travel & holiday, clothes, books, tickets, films, music, software, food) QB1b Which of the following activities do you also do on the Internet? (ONLY IF "YES" in QB1a.3) Purchase goods or services from a seller located in (OUR COUNTRY).
Purchase goods or services from a seller located in another EU country.
Purchase goods or services from a seller located outside the EU.

Table 4. Purchase of good and services online in Member States vs. other locations

		In EU		Outside EU	
		Yes	No	Yes	No
In MS	Yes	16%	30%	11%	35%
	No	2%	52%	2%	52%
In EU	Yes			9%	9%
	No			4%	78%

Base: Internet users.

Source: QB1a & QB1b.

Table 5. Factor analysis of activities carried out on the Internet

	Factor 1. Social activities	Factor 2. Transactions	Factor 3. Software activities
Use a social networking site	.78		
Use a sharing site	.75		
Instant Messaging	.71		
VoIP	.41		
Home banking		.79	
eCommerce		.68	
eGovernment		.68	
Own website			.69
Browser plug-ins			.59
Blog			.58
Cloud software		.32	.50
Peer-to-peer software	.42		.46
Auto values	2.88	1.67	1.08
% Variance explained	24	14	9

Source: QB1a & QB1b.

Base: Internet users.

Notes: Rotated components matrix; factor analysis by main components; Rotation: Varimax with Kaiser-Meyer-Olkin 0.781; Bartlett's test of sphericity p=0.000; Convergence in 4 iterations; Minimum eigenvalue 1; Values below .03 are omitted.

Within this figure, the bulk of eCommerce occurs within Member States (46% of all Internet users); there are very limited online purchases cross border and very little difference between percentages of people buying inside and outside the EU (18% and 13% respectively).[8] The notion of EU single digital market is still absent in users' Internet activities. Also notable is the relation between different locations of eCommerce. National eCommerce strongly underpins both in-EU and out-EU eCommerce: virtually nobody shops in-EU and out-EU without shopping in their own country [Table 4].

Also, eCommerce activities are most similar to other 'transactional' activities [eServices], generally carried out within one own country – home banking and eGovernment [Table 5]. It may well be that eServices are a 'single bundle' in people's eyes and experience. This may also mean that the three activities may grow together, if proper interoperable systems are provided that make it easier to transact elsewhere [outside one's country]; the question remains open whether eCommerce could assist eGovernment, which currently very low in EU27 [23% of Internet users].

Factor analysis was conducted to see whether each of the possible places where people shop online were akin to other Internet activities [table not reported]. People shopping online in their own countries also tend to do home banking and eGovernment, while people who shop in the EU and outside the EU tend to do that alone, as a separate activity [which, strangely, co-occur with advanced software behaviour]. This confirms the different nature of eCommerce in MS and across MS: more ingrained in the national Internet experience the former, building on national eCommerce and more advanced the latter.

8 These numbers are confirmed from findings by the DAE scoreboard: "Fragmentation also limits demand for cross-border eCommerce transactions. Less than one in ten eCommerce transactions are cross-border, and Europeans often find it easier to conduct a cross-border transaction with a US business than with one from another EU MS."

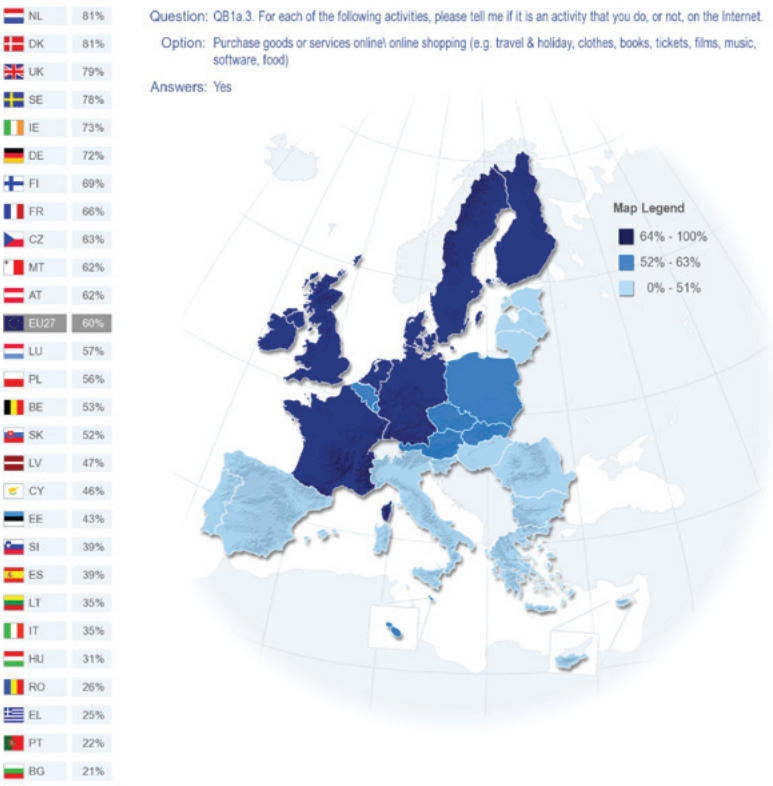
To further test this concept, we crossed cross-border eCommerce and MS-based eCommerce by frequency of Internet use (a proxy for Internet expertise), and with overall number of Internet activities carried out. The assumption was that both indicators are better predictors of cross-border eCommerce than of MS-based eCommerce. We also looked at general socio-economic characteristics and at regulatory references.

We found that males are those who shop primarily from outside the EU, and slightly more cross-border; as we expected, frequent Internet users shop slightly more across borders; the strongest predictor is the overall number of Internet activities carried out. First, it has a significant, strong correlation with the number of contexts where people shop [Pearson's r = .36]. Thus people who do more online in general also shop in more contexts – MS, cross-border, non-EU. Second, there is a small difference on top of this regarding where people shop: more activities are more strongly related further distance of eCommerce [eta respectively .28, .29, .30]. Finally, people shopping online in different places have remarkably similar regulatory preferences concerning the protection of personal data – specifically all support to a large degree the need for coherent regulation of data disclosure in eCommerce.

2.4 National differences in eCommerce

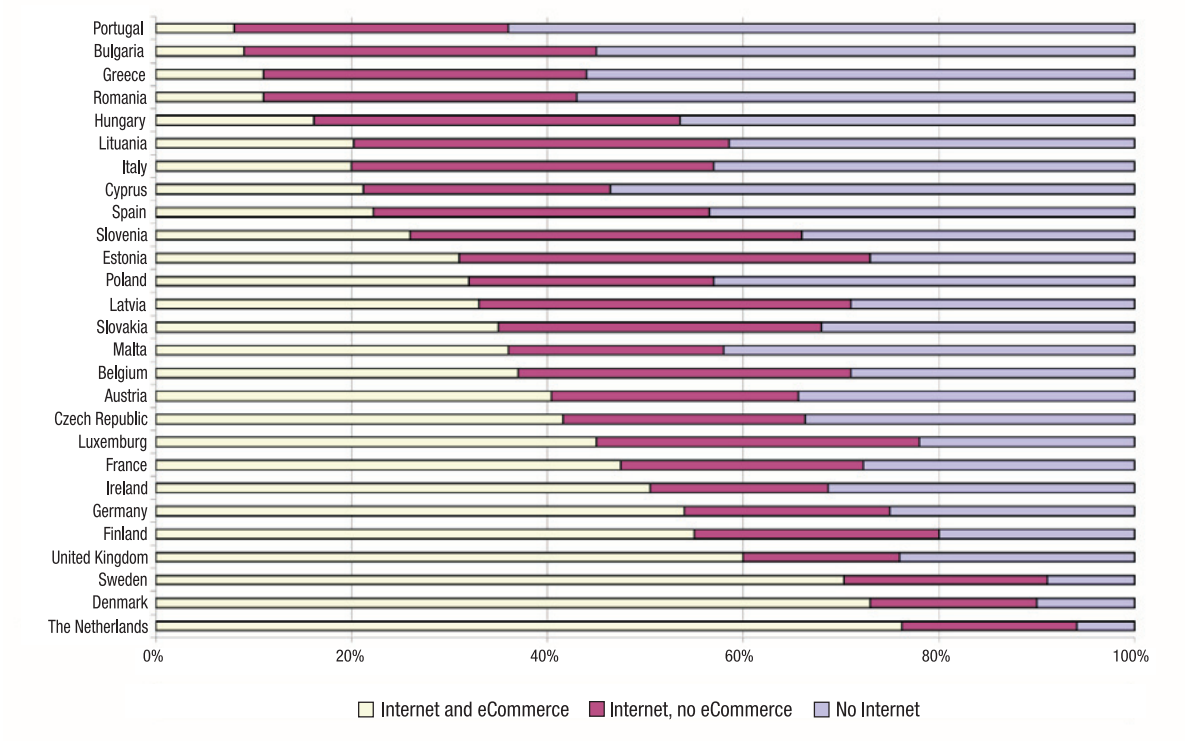
While a large majority of European Internet users purchase goods or services online (60%), the uneven take-up of eCommerce in MS is striking. A high percentage of respondents shop online in northern and western Member States: Denmark and the Netherlands (81%), the United Kingdom (79%), Sweden (78%), Ireland (73%), Germany (72%) and Finland (69%). In contrast, respondents in the south and east are least likely to purchase online: Bulgaria (21%), Portugal (22%), Greece (25%) and Romania (26%).

Figure 1. eCommerce by country



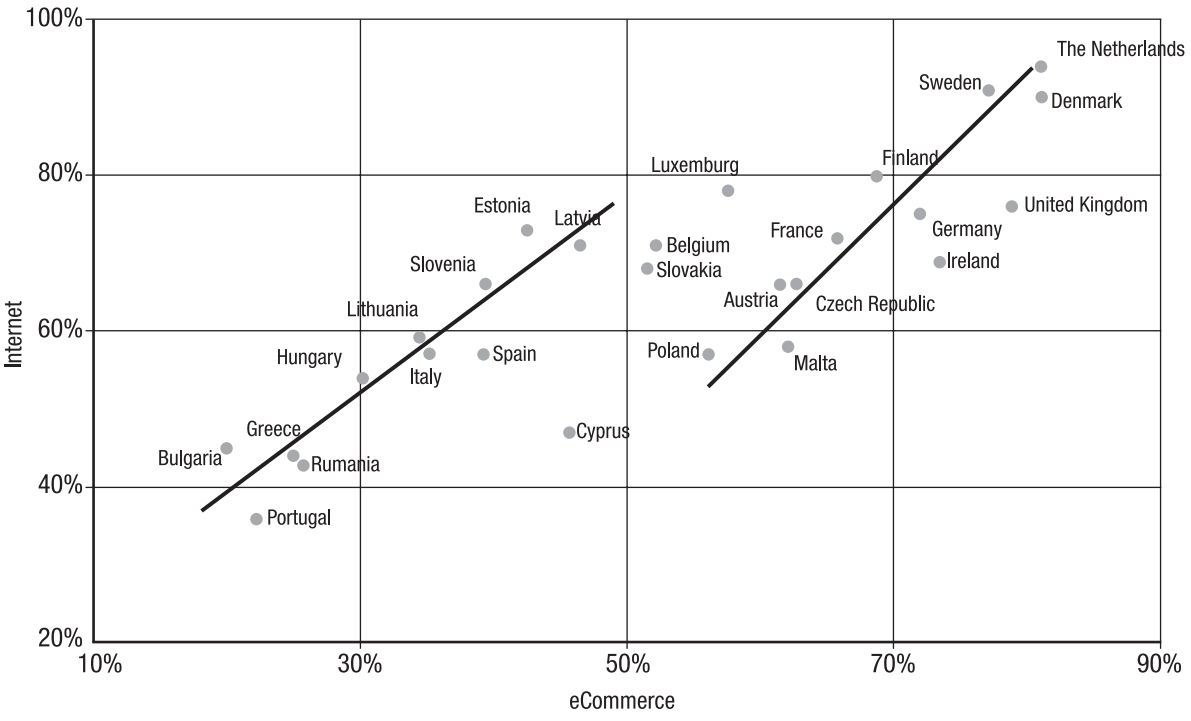
Source: QB1a.3.
Base: Internet users (66% of total sample).

Figure 2. Internet use and eCommerce by country



Source: QB1a.3 crossed by D62.
Base: EU27.

Figure 3: Country scatter plot of Internet use and eCommerce



Source: QB1a.3 crossed by D62.
Base: EU27.

Figure 4. Socio-economic profile of eCommerce users

Purchase goods or services online/ online shopping (e.g. travel & holiday, clothes, books, tickets, films, music, software, food)

	Yes	No	DK
EU27	60%	40%	-
Sex			
Male	62%	38%	-
Female	57%	43%	-
Age			
15-24	54%	45%	1%
25-39	66%	34%	-
40-54	60%	40%	-
55 +	55%	45%	-
Education (End of)			
15-	42%	58%	-
16-19	57%	43%	-
20+	70%	30%	-
Still studying	55%	44%	1%
Household composition			
1	59%	41%	-
2	61%	39%	-
3	59%	41%	-
4+	59%	41%	-
Respondent occupation scale			
Self-employed	64%	36%	-
Managers	75%	25%	-
Other white collars	61%	39%	-
Manual workers	60%	40%	-
House persons	60%	40%	-
Unemployed	48%	52%	-
Retired	50%	50%	-
Students	55%	44%	1%
Use of the Internet			
Everyday	69%	31%	-
Often/ Sometimes	35%	64%	1%
Never	-	-	-
Difficulties paying bills			
Most of the time	54%	46%	-
From time to time	53%	47%	-
Almost never	65%	35%	-

Source: QB1a.3.
Base: Internet users.

Furthermore, at country level, there is a strong correlation between rate of Internet use and proportion of people shopping online. In Figure 2 we show how Internet use and eCommerce relate across EU27. The proportion of people shopping online [yellow bar] increases rapidly vs. people not buying online [red bar] as Internet access increases [the shorter the blue bar gets]. This is also evident looking at the grey dot distribution in Figure 3, showing a very strong relation [r = 0.79] between eCommerce and Internet use across EU27. This is not intuitive: one may think that, given Internet access, people in different countries will have the same propensity to shop online. This is not so: there appears to be two groups of Europeans: one at a lower level of eCommerce, and the other at a higher level of eCommerce [two distinct lines in Figure 3]. For both blocks there is an almost perfect correlation between Internet use and eCommerce. This we interpret to mean that there are national factors that influence eCommerce uptake – supply, structure of the digital market, or regulation [these are well explained by existing evidence, recently summarised in the DAE scoreboard].[9]

There are also other factors such as that Internet use and eCommerce have common roots, namely the socio-economics underpinning Internet uptake [affluence, education, age], which also strongly influence online shopping [Figure 4]. We may think of this as a funnel

9 http://ec.europa.eu/information_society/digital-agenda/scoreboard/index_en.htm

that gets narrower the more the people get into sophisticated and financially costly behaviours [such as eCommerce; the same happens, with different variables into play, for political participation online].[10] Overall, the typical eCommerce user is older (25-55), typically male, better educated, heavy Internet users, in management positions or self-employed and generally more affluent. When one compares this profile to the typical SNS user profile, who is more likely to be younger, typically female, well educated, a heavier Internet user and is still studying or is unemployed, it is rather obvious that these profiles are distinct.

This adds a note of caution to the interpretation of results, beyond usual considerations of statistical significance of small samples. For eCommerce, socio-economic characteristics of respondents may explain results more accurately than country of residence. Especially, this is true of countries with lowest Internet penetration and lower uptake of eCommerce [Portugal, Bulgaria, Greece, Rumania, Hungary] and lower GDP, and of countries with highest Internet penetration and eCommerce rates [Sweden, Denmark, the Netherlands] and higher GDP. In turn, looking at these blocks separately may help determine the weight of cultural determinants of online shopping, including identity and data protection behaviours and perceptions.

2.5 Personal data disclosure in eCommerce[11]

Then, questions were asked directly regarding disclosure, identity management and data protection in eCommerce. Around nine out of ten respondents reveal their name (90%) and their home address (89%) on eCommerce sites [Table 6]. In addition, almost half give mobile phone number (46%), and a third their nationality (35%) or financial information such as salary, bank details and credit record (33%). Almost one in five give national identity number, identity card number, or passport number (18%). There is a thus common core of disclosure of name and address, to lesser extent nationality and mobile number.

Very few people, 6% share their activities in the context of eCommerce [willingly or at least consciously]. As this information is not normally asked by eCommerce sites, the low number is understandable. People share their activities elsewhere, such as in Social Networking Sites, and they may move onto eCommerce sites based on the preferences expressed there; advertising seems to be an increasingly important selling point for SNS and an important source of revenue.

This may also mean that traditional eCommerce vendors may have been less rapid that SNS companies to see the value of web2.0 for offering to customers products [generally digital, such as music, but not only] tailored to and anticipating their preferences. If this is the case, which need to be further probed by a market survey, then again European eCommerce companies and sites [which are where most people buy] may be at a competitive disadvantage vis-à-vis largely US-owned SNS sites.[12]

Factor analysis consolidates these results [Table 7]. There are four main types of information people disclose 'jointly': social information, biographical information, sensitive information and security-related information. It is interesting that financial information does not belong in the security group, but in the sensitive information group. This pattern of behaviour may be good news for those wishing to create a disclosure

10 Lusoli, W. (2012). Voice and equality that state of electronic democracy in Britain. Cresskill, NJ: Hampton Press.

11 QB4b Thinking of the occasions when you have purchased goods or services via the Internet, which of the following types of information have you already disclosed?

12 With the obvious exception of Amazon, for instance, again US-owned, that makes large use of collaborative filtering based on previous purchasing behaviour and click-stream data.

Table 6. Personal data disclosed in eCommerce

	% of eCommerce users
Name	90
Address	89
Mobile number	46
Nationality	35
Financial	33
National identity number	18
Activities	6
Work history	5
Preferences	5
Photos	4
Websites visited	4
Medical information	3
Friends	2
Fingerprints	2
Other	1
None	2
Don't know	1

Source: Qb4b.

Base: Internet users who purchased good or services online.

Table 7. Factor analysis of personal data disclosed on eCommerce sites

	Factor 1. Social information	Factor 2. Biographical information	Factor 3. Sensitive information	Factor 4. Security information
Friends	.715			
Photos	.708			
Preferences	.697			
Activities	.649			
Websites	.620			
Address		.823		
Name		.809		
Financial			.722	
Medical info			.613	
Fingerprints			.593	
Employment			.361	
Identity number				.760
Mobile number				.582
Nationality				.493
Auto values	2,98	1,94	1,28	,98
% Variance explained	21,2	13,9	9,1	7,0

Source: Qb4b.

Base: Internet users who purchased good or services online.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0.749; Bartlett's test of sphericity p=0.000; Convergence in 3 iterations; Minimum eigenvalue .98.

systems based on third-party credentials, rather than on direct disclosure of bank or credit related information.

2.5.1 Personal data disclosure in eCommerce by country and socio-economic status

The similarity between MS in relation to personal disclosure of what was defined as 'biographical data' (name, address) is truly remarkable [Table 8].

On the one hand, this may reflect homogenous, well-established transactions that require standard information; on the other, the similarity of user experience with disclosure of core data while shopping online should allow for significant harmonisation and, should problems exist (and they do exist, we argued above), be addressed across EU27, by either technical (identity by design, credential cores) or legal means (harmonisation, standards, …).

Table 8. Disclosure of personal data by country

	Name (%)	Address (%)	Mobile number (%)	Nationality (%)	Financial (%)	Identity number (%)
EU27	90	89	46	35	33	18
Austria	90	85	55	60	34	11
Belgium	94	88	44	52	26	18
Bulgaria	84	79	42	29	16	25
Cyprus	92	80	36	43	31	13
Czech Republic	94	94	71	17	13	13
Denmark	96	91	73	49	56	32
Estonia	90	82	65	23	19	47
Finland	95	95	67	46	34	38
France	93	93	51	31	44	9
Germany	92	92	30	51	32	12
Greece	93	83	45	30	24	22
Hungary	93	85	59	15	36	19
Ireland	94	90	55	56	41	5
Italy	69	67	34	27	21	32
Latvia	93	85	71	11	28	57
Lithuania	84	76	51	16	14	19
Luxemburg	93	91	47	34	47	18
Malta	86	95	25	74	30	17
Poland	91	90	64	17	6	13
Portugal	72	60	26	26	19	23
Rumania	76	67	45	29	17	33
Slovakia	90	90	71	20	19	23
Slovenia	95	89	61	19	26	20
Spain	88	74	43	46	38	51
Sweden	96	94	76	35	26	72
The Netherlands	98	96	55	42	37	20
United Kingdom	89	92	42	24	39	5

Source: QB4b.

Base: Internet users who purchased good or services online.

Notes: Table reports % of people disclosing personal data items in EU27 and in individual MS.

Other items, largely of social and sensitive nature, are not reported as they are below 6%.

Table 9. Disclosure of personal data categories by country

	Social information	Biography information	Sensitive information	Security information
EU27	0.04	0.01	0.06	0.21
Austria	0.46			
Belgium			-0.07	
Bulgaria		-0.39	-0.26	
Cyprus				-0.07
Czech Republic			-0.44	0.09
Denmark	-0.30	0.26	0.19	0.49
Estonia	-0.11	-0.37	-0.19	0.65
Finland	-0.21	0.14	-0.08	0.58
France		0.24		-0.21
Germany		0.14		-0.14
Greece	0.54	-0.12	-0.23	-0.02
Hungary	-0.11			0.01
Ireland	0.23	0.26		-0.05
Italy	0.35	-0.93	0.21	
Latvia	-0.24	-0.26	-0.22	0.76
Lithuania		-0.44	-0.35	0.01
Luxemburg	-0.19	0.17		-0.05
Malta		0.14		0.05
Poland	-0.12	-0.17	-0.49	0.08
Portugal	0.31	-0.97	0.17	-0.02
Rumania	-0.11	-0.77	-0.11	
Slovakia			-0.35	
Slovenia			-0.26	0.03
Spain	0.14	-0.37	0.18	0.62
Sweden	-0.38		-0.23	1.19
The Netherlands		0.28		
United Kingdom				-0.38

Source: QB4b.

Basis: Internet users who purchased good or services online.

On the other hand, however, there are differences across regional blocks, rather than across individual MS for other personal data, such as mobile phone and nationality. We noted that regional differences in the disclosure of personal data may be due to the uneven 'culture' of eCommerce across EU27. In fact, Internet shoppers in the Nordic countries and in Eastern Europe are the most likely to have given their mole phone number. But nationality is given largely in Nordic country, while far less so in Eastern Europe. A second exception regards the disclosure of identity numbers, which varies considerably across MS. Such variety may have to do with identity-related legislation in different member states and constitutes a significant barrier for the deployment of both technical and legal interoperable systems in the EU (within eCommerce).

To provide a more structured view on the results, we looked at country differences in the provision of 'clusters' of personal data, as they were determined using factor analysis: biography, social, sensitive and security related [Table 9]. There is a slight difference between north and

Table 10. Disclosure of personal data categories by socio-economic status

		Financial (%)	Identity Number (%)	Name (%)	Address (%)	Nationality (%)	Mobile Number (%)
	EU27	33	18	90	89	35	46
Terminal education age	15-	28	15		83		37
	16-19		15		89		
	20+	36	22		91		49
	Still Studying				87		
Age [brackets]	15-24						51
	25-39	37					49
	40-54						47
	55+	28					35
Occupation	Self-employed	27	22				51
	Managers		20				
	Other white collars		20				50
	Manual workers	38					
	House person	40	12				
	Unemployed	36					51
	Retired	26	13				33
	Students	30					
Personal mobile phone	No			77		29	21
	Yes			90		36	47
Difficulties to pay bills	Most of the time	38					
	From time to time	36					
	Almost never/ never	31					

Base: Internet users who purchased good or services online.

Notes: Only significant differences at $p < 0.01$ are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

south of Europe as to the provision of social information, which is however provided very seldom in eCommerce. Conversely, there is more variance across MS regarding the provision of security-related information. Increasingly more often, eCommerce sites make use of authentication techniques based on identity number, mobile number (via SMS) and other ways of pegging 'virtual identity' to real identity.

This type of disclosure, which we interpreted as security-related, is highest in countries with established systems of electronic authentication, such as Austria, Belgium, Spain, Finland, The Netherlands and Sweden. Possibly, there is a case for extending this practice to other countries, and to other possible credentials (such as name and address), via burgeoning effort of identity credentials, which may well work cross-borders.[13]

In terms of socio-economic status, education appears to play a role in the disclosure of some information [Table 10]. Online shoppers who

13 More analysis is required of this aspect, by means of micro-macro data integration.

studied until the age 20 or later are more likely to disclose home address (91%), financial information (36%), mobile phone number (49%) than those who finished school before the age of 16 (respectively 83%, 28%, 37%). In general, we found three main patterns:

1 Older people, generally with lower levels of formal education, tend to disclose less information of different types; younger people are more likely to disclose mobile number.

2 Ownership of mobile phones makes a difference to security-related disclosure.

3 Less affluent people tend to disclose slightly more financial information.

2.5.2 Disclosure of data in relation to what is personal and reasons for disclosure[14]

We then crossed disclosure of data with perception that this data is actually personal [Table 11]. This tells us whether people who disclose personal data consider it as such.[15] Results are very surprising, in two respects. First, overall, there is no apparent relation between considering one's data personal and disclosing it on eCommerce sites. So even if people consider information personal, still they disclose it. This may indicate that there is no real alternative available to people other than disclose this information (they are "forced" to disclose such data).[16]

Table 11. Data disclosure in eCommerce crossed by what is personal data

Data disclosed		Consider it personal
Financial	No	82%
	Yes	90%
Identity number	No	78%
	Yes	76%
Name	No	34%
	Yes	47%
Address	No	49%
	Yes	63%
Nationality	No	28%
	Yes	35%
Mobile number	No	62%
	Yes	66%

Source: Qb4b by Qb2.

Base: Internet users who purchased good or services online.

Notes: Only items disclosed by more than 6% of people are reported.

14 QB2: Which of the following types of information and data that are related to you do you consider as personal?

15 Questions were asked in an order that does not influence the responder they first asked what information is personal data, and then what has been disclosed.

16 The principle of privacy by design implies that IDM systems should allow for anonymous and pseudonymous interactions in the context of commercial transactions (service providers within the commercial sector do not need to receive clients' extensive identity information that they currently demand).

Table 12. Reasons to disclose personal data in eCommerce

	% of eCommerce users who disclose information
To access the service	79%
To obtain a service adapted to your needs	27%
To save time at the next visit	19%
To benefit from personalised commercial offers	13%
To receive money or price reductions	12%
To get a service for free	11%
To connect with others	6%
For fun	2%
Other	3%
DK	1%

Source: Qb5b.

Base: eCommerce users who disclosed personal data.

Second, and more surprising, for many items [name, address, nationality, financial information], there is a positive relationship; that is the more people consider this information personal, the more they disclose it on eCommerce sites [!]. This may mean that this information takes on personal connotation for people when it is disclosed, rather than having 'a priori' personal value. In this case, a system of credentials where no face-value information is disclosed may help people perceive that the information they have disclosed is 'procedural' rather than personal.

Part of the reason may also be that, in order to shop online, some information has to be disclosed, regardless of whether it is considered as personal. Indeed, the most important reason for disclosing personal information when shopping online mentioned by a vast majority of online shoppers is to access the service (79%) [Table 12]. This reason is followed at a distance by to obtain a service adapted to their needs (27%), and to save time at the next visit (19%). It is interesting that the reason to disclose is largely functional: accessing the service [thus dependent on what information is asked], and to save time. Customisation of the service [which however includes an element of convenience] and personalised offers based on profiling lag far behind as reasons to disclose.

Also, there is no clear link between information disclosed and reasons for disclosing, beyond small predictable variations concerning 'needed' information for dispatch, contact information etc [Table 13]. Financial information is offered for functional reasons [access service, save time], name and address to access the service, nationality for a range of reasons. Overall, our analysis portrays a picture that is not overtly favourable to the deployment of customised services based on the enhanced [and increased] disclosure of personal data.

2.5.3 Reasons for disclosure, country and socio-economic status

Above we noted that a sizeable minority of those disclosing nationality, mobile and identity number do so to benefit from personalised commercial offers or to obtain a service adapted to their needs.

We examine here the residence and socio-economic characteristics of people who disclose for those reasons [Table 14]. While there are no clear regional patterns, a few countries stand out. First, people in Germany, Austria, Slovakia and Slovenia are more likely to share to obtain a better service. Second, people in The Netherlands and in the UK are far less likely than other Europeans

Table 13. Data disclosure crossed by reason to disclose personal data

		Financial	Identity #	Name	Address	Nationality	Mobile #
To access the service	No	29%	18%	85%	83%	33%	38%
	Yes	35%	19%	95%	94%	37%	50%
To save time at the next visit	No	32%	17%	93%	92%	35%	46%
	Yes	39%	22%	93%	91%	45%	55%
To benefit from personalised commercial offers	No	33%	17%	93%	92%	36%	46%
	Yes	36%	27%	90%	88%	41%	56%
To obtain a service adapted to your needs	No	33%	17%	92%	91%	34%	47%
	Yes	35%	21%	94%	93%	44%	48%

Source: qb4b by Qb5b.

Base: eCommerce users who disclosed personal data.

Notes: The table reports % of people disclosing items of information in relation to reasons why information is disclosed.

Table 14. Reason to disclose personal data by country

	To obtain a service adapted to your needs (%)	To benefit from personalised commercial offers (%)	To connect with others (%)
EU27	27%	13%	6%
Austria	38%		
Bulgaria	40%		
Cyprus		24%	10%
Czech Republic			
Finland	35%	24%	
France		21%	
Germany	43%		10%
Greece		49%	
Hungary		22%	
Italy		24%	
Latvia		7%	
Lithuania	44%		
Malta	42%		
Poland	18%		
Portugal	15%	29%	
Rumania		23%	
Slovakia	38%	20%	10%
Slovenia	38%		
The Netherlands	19%	6%	2%
United Kingdom	10%	4%	

Source: Qb5b.

Base: eCommerce users who disclosed personal data.

Notes: Only significant differences at $p < 0.01$ are reported [i.e. when there is a 99% probability that the relation reported is not due to chance]. Differences from average were not significant for LU, ES, SW, DK, EE, BE, IE.

to disclose for reasons other than to access the service [what we may call a pragmatic attitude regarding disclosing data in eCommerce].

Regarding socio-economics, reasons to disclose remain stable across most characteristics [table not reported]. However, young people disclose more to connect with others; and mobile phone users disclose more to obtain a service adapted to their needs.

2.6 Risks, control and responsibility on data disclosed in eCommerce

2.6.1 Risks of eCommerce disclosure[17]

We then examined personal data disclosure in direct relation with perceived risks of such disclosure; with control on the data disclosed; and with responsibility concerning the safe handling of the data disclosed. Many risks are reported by respondents [procedural, substantive, related to safety, related to reputation], and no clear picture emerges from dimensional reduction via factor analysis [e.g. risks are relatively unrelated and they form no visible pattern]. In the main, fraud (55%), stealth use of and stealth sharing of one's information with a third party (both at 43%), and identity theft (35%) are the risks most frequently reported. Risks to reputation and to personal safety are mentioned by far fewer respondents [Table 15].

We thus crossed frequently mentioned risks by different modes of eCommerce [in-MS, in-EU, out-EU]. Perceptions of risks do not vary significantly across purchase contexts [Table 16]; perception of data protection risks may be as much a barrier to cross-border eCommerce as it is

Table 15. Risks from disclosing personal data in eCommerce

	% of service users who disclose personal data
Yourself being victim of fraud	55
Your information being used without your knowledge	43
Your information being shared with third parties without knowledge	43
Your identity being at risk of theft online	35
Your information being used to send you unwanted commercial offers	34
Your information being used in different contexts	27
Your personal safety being at risk	12
Your reputation being damaged	4
Your views and behaviours being misunderstood	4
Yourself being discriminated against	3
None	2
DK	1
Other	0

Source: Qb7b.

Base: eCommerce users who disclosed personal data.

17 QB7b: I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of your personal information to buy goods or services via the Internet?

Table 16. Risks from disclosing information in eCommerce crossed by eCommerce location

	% of reported risks		
	Buy goods in own country	Buy goods in EU	Buy goods outside EU
Yourself being victim of fraud	57%	57%	61%
Your information being used without your knowledge	45%	42%	42%
Your information being shared with third parties without knowledge	45%	48%	43%
Your information being used to send you unwanted commercial offers	36%	36%	35%
Your identity being at risk of theft online	37%	36%	39%
Your information being used in different contexts	28%	28%	25%

Source: Qb7b by Qb1b.

Base: eCommerce users who disclosed personal data.

to national eCommerce. Thus reasons other than risk perceptions in relation to disclosure hamper cross-border eCommerce. A few of these reasons were identified in previous surveys,[18] such as security concerns, language and lack of supply of cross-border eCommerce. More detailed analysis of attitudes to risks, crossing with surveillance, concern for over exposure of personal data on the Internet and profiling questions to detect similarity is proposed in the last section of this chapter.

Risks by country and socio-economic status

There is no clear pattern of risks at country level, as respondents mention different combinations of risks in different countries [Table 17]. The same is true of socio-economic traits [table not reported], with some minor variance. First, young people again stand out, in that they are slightly more worried about personal safety, and less about their information being shared with third parties without them knowing or in different contexts than the original. Second, people owning personal mobile phones are more concerned about their information circulating without them knowing, and about fraud.

2.6.2 Control on personal data disclosed in eCommerce[19]

We examined the degree of control people perceive to have on personal data they have disclosed on eCommerce sites. Less than one in five thinks they have total control on their own information [Table 18]. About one in three thinks they have no control at all. About half think they have some control. This may be normal, as except for large eCommerce portals such as eBay, for most online purchases people do not have a profile page available to them, or a single point of entry or a purchase history (what they bought in past interaction, what they searched for, offers looked at). Further to this, we found that people feel slightly less in control when they disclose more of their biographical information [r = -0.1]. This may make it harder for people to feel in control of personal data they have disclosed one-off, several times on different sites.

One may speculate on the relative merits of a tool that allowed a degree of personal data integration, for the benefit of the buyer rather than of the seller. Of course, any such 'control' tool would need to comply with the a priori principle of data minimization, and help organise information

18 See http://ec.europa.eu/consumers/strategy/facts_en.htm.

19 QB6b: How much control do you feel you have over the information you have disclosed when shopping online, e.g. the ability to change, delete or correct this information?

Table 17. Risks from disclosing information in eCommerce by country

	Yourself being victim of fraud	Your information being used without your knowledge	Your information being shared with third parties without knowledge	Your identity being at risk of theft online	Your information being used to send you unwanted commercial offers	Your information being used in different contexts	Your personal safety being at risk
EU27	55%	43%	43%	35%	34%	27%	12%
Austria	42%		54%	20%	42%		
Belgium	43%				45%		
Bulgaria	36%	67%	31%	22%		11%	
Cyprus		64%				18%	28%
Czech Republic	41%			19%	48%		
Denmark						40%	
Estonia				30%		6%	26%
Finland						43%	24%
France	71%			43%		17%	
Germany			59%	24%		41%	
Greece		51%		22%			
Hungary	42%	51%			48%	15%	
Ireland		59%		52%		11%	22%
Italy	33%		34%	25%			
Latvia		52%		19%		14%	
Lithuania				16%		11%	
Luxemburg					42%		
Malta			34%		23%	15%	
Poland				24%			
Portugal			25%	25%	24%		
Rumania	27%	60%	27%			8%	
Slovakia	38%					17%	26%
Slovenia		53%	40%	22%			20%
Spain		35%	29%		21%	17%	26%
Sweden	68%			46%			7%
The Netherlands	36%		55%		56%		4%
United Kingdom	65%	34%	33%	56%	22%		

Source: Qb7b.

Base: eCommerce users who disclosed personal data.

Table 18. Control over information disclosed in eCommerce

	% of service users who disclose information
No control at all	30
Partial control	50
Complete control	18
DK	2

Source: Qb6b.

Base: eCommerce users who disclosed personal data.

that is strictly necessary for the transaction, rather than elicit further personal data.

Control on data disclosed by country and socio-economic status

People from a group of countries from the south and east of Europe [Portugal, Malta, Cyprus, Hungary, Poland, Italy] has a higher perceived control on personal data disclosed; conversely, the one, single country were people feel far less in control is Germany [Table 19]. From previous analysis [Table 17], we also gather that Germans perceive particularly high risks of mishandling of their personal data by third parties. Germany, in fact, is where people may have the greatest awareness of their information rights, as they are protected by the constitutional principle of informational self-determination. Whether the perception of a right in relation to protecting one's own personal data correlates with perceived lack of control is however to be tested. We will test later whether perceived control has a positive or negative effect on the practical measures people take to protect their identity online. Regarding socio-economic status, unmarried, young people who are still studying have the highest perceived control on the data they disclose in eCommerce. There are very limited differences outside this social group. Overall, perceived control can be explained jointly by residence, as described, and by young age.

Table 19. Control over information by country

	No control at all	Partial control	Complete control	% of young people in country
EU27	30%	50%	18%	15 %
Portugal	11%	66%		17%
Hungary	11%	60%	28%	14.5%
Malta	12%		43%	17.5%
Cyprus	15%	37%	48%	19%
Ireland	17%	62%		19%
Poland	18%	58%		17.5%
Italy	23%		29%	12%
Germany	42%		9%	13%

Source: Qb6b.

Base: eCommerce users who disclosed personal data.

2.6.3 Responsibility for safe handling of data disclosed[20]

Turning to responsibility for the protection of personal data once it's been disclosed, a minority of eCommerce users (20%) consider public authorities responsible [Table 20]. But about the same proportion (40%) argue that they or companies are responsible to keep their personal data safe. Very few people claim that they do not know. Also, two thirds of people who say they are primarily responsible also think that online sites are responsible in the second place [Table 21]. The reverse does not hold, as people who think shopping sites are primarily responsible also see a secondary, equal role for themselves and authorities. Overall, abut one in two respondents do not see public authorities as having either primary or secondary responsibility for protection of personal data safety.

20 QB8b1: Who do you think should make sure that your information is collected, stored and exchanged safely when you buy goods or services via the Internet? Firstly? QB8b2: And secondly?

Table 20. Overall responsibility for personal data safety in eCommerce

	% of eCommerce users	
	Firstly	Secondly
You	41	27
The site owners	39	37
Public authorities	19	33
Other	0	1
DK	1	2

Source: Qb8b.

Base: eCommerce users.

Table 21. Conjoint responsibility for personal data safety in eCommerce

		Responsibility secondly	
Responsibility firstly		Column %	Total %
You (41%)	The online shopping sites	64%	26%
	Public authorities	36%	15%
The online shopping sites (39%)	You	51%	20%
	Public authorities	49%	19%
Public authorities (19%)	You	37%	7%
	The online shopping sites	63%	12%

Source: Qb8b.

Base: eCommerce users.

However, we found significant differences in perceived responsibility by the level of perceived control [Table 22]. Indeed, people who think they have no control on their personal data [again: once they've been disclosed], tend to see higher co-responsibility of industry and regulators. Conversely, those who think they have total control tend to see joint self-company responsibility. In all cases, companies are seen as responsible regardless of level of perceived control [e.g. their conferred responsibility remains relatively stable across perceived control]. Finally, the more people disclose what we defined as 'biographical data', the more they think responsibility lies with online shopping sites and regulators [table not reported].

Responsibility by country and socio-economic status

People in different countries attribute different responsibility[21] concerning the protection of personal data shared in eCommerce to themselves, companies they deal with and authorities [Table 23]. So, in Italy and in Spain people attribute more responsibility to

21 For clarity in this section, we use a single composite measure of responsibility; we give a value of '2' to people who attribute first responsibility to any of the agents mentioned [self, site, authorities]; and a value of '1' to people who attribute secondary responsibility to these agents. Then, we check this measure for every agent against country of residence and socio-economic traits.

Table 22. Conjoint responsibility by level of control on personal data disclosed

Responsibility firstly	Responsibility secondly	Total control	Partial control	No control
You	The online shopping sites	34%	28%	20%
	Public authorities	14%	15%	13%
The online shopping sites	You	23%	21%	18%
	Public authorities	17%	18%	24%
Public authorities	You	5%	7%	9%
	The online shopping sites	6%	11%	17%
Totals		100%	100%	100%

Source: Qb8b.

Base: eCommerce users.

Table 23. Responsibility to protect personal data by country

	Self	Company	Authorities
EU27	1.1	1.2	0.7
Denmark	.9		
Spain			1.1
Ireland	1.4		
Italy	.9		1.1
The Netherlands		.9	
Sweden	.8	1.5	
United Kingdom			.5
Slovenia	1.3		.4

Source: Qb8b.

Base: eCommerce users.

Note: Results reported are total weighted scores for responsibility, where first responsibility to the agents [self, site, authorities] is attributed a value of '2'; and a value of '1' goes to secondary responsibility.

authorities, while UK and Slovenian residents much less so. Company responsibility is seen of highest priority in Sweden and lowest in the Netherlands. Concerning individual responsibility, Irish and Slovenian residents rank it highest, while it is lowest Sweden, Denmark and Italy. Apart from telling an interesting tale about regulatory preferences, these results give important indication of people's willingness of to protect themselves in online transactions, beyond socio-demographic traits. Indeed, there are very small differences in attributing responsibility based on socio-economic traits. The only discernible pattern concerns younger people [especially young females], who tend to indicate companies rather than authorities as responsible for protecting the personal data they disclose. Conversely, retired and older people tend to attribute responsibility in the reverse order.

2.7 Relations with other variables

Fist, we checked 'disclosure' in relation to a number of other data form the survey, specifically identity-relevant questions and regulatory questions. The idea is that identity systems may mitigate or compound some of the issues in relation to disclosure (over-disclosure, perception of risks, degree of control, for one). Results are reported descriptively below; all coefficients are reported in Table 25.

2.7.1 Disclosure

First, data shows that disclosure behaviour is related to other Internet behaviours, rather more strongly than it is related to attitudes towards disclosure. That is: the steering of certain desired behaviours in terms of disclosure depends more on 'behavioural' remedies and tools than with greater awareness and enhanced perceptions, especially of risks. More specifically, disclosure behaviour is associated with

- Use of credentials in daily life [business related: r = .23]; people who disclose biographical information also use credentials such as credit cards and customer cards in their daily lives. But these credentials are much less strongly associated with the disclosure of sensitive information and security information. Government-issued credentials have a much lower correlation with disclosure of personal data. This finding is explored below in more detail.

- Identity protection behaviours [do not disclose: r = .18; adjust: r = .19]; people who disclose more biographical information also minimise what they disclose and adjust the information according to context as coping strategies in daily life, online and offline. Provision of security information is also to some extent adjusted to context. This may be good news for enforcing the principles of data minimisation of purpose-binding.

- Internet identity protection [r = .17]. The more people disclose biographical information online, the more they try to stay protected online using a range of strategies. Again, this may be good news for those interested in developing tools allowing people to protect their data. This is consistent with the relation discussed above between disclosure and control.

Beyond actual behaviours, disclosure behaviour in eCommerce is related to:

- Possibility to delete personal data [r = .13]; people who disclose more biographical information would like to be able to delete personal data whenever they want.

- Awareness of identity theft and data loss [media awareness: r = .10, social awareness r = -.08]; people who disclose more biographical information tend to be more aware of issues of identity theft and data loss through the media; but they also tend to be less socially aware of the same issue (i.e. it has not happened to people they know). What seems to be happening is increased general awareness for people disclosing less sensitive information, and increased, specific awareness (social, family) for people disclosing sensitive and security information.

2.7.2 Disclosure and credentials in eCommerce

We noted above that those who use a number of identity credentials are more likely to disclose biographical info, mainly name and address in eCommerce. This is natural for travel reservations, for delivery details and miscellanea for other service-specific reasons. And that bank cards and credit cards are at the centre of the system of disclosure, again a fact we are familiar with, as credit cards underpin the structure of today's eCommerce. More interestingly: credit cards and store cards are also linked to the disclosure of information people consider as sensitive, while this is not the case for other credentials [Table 24]. A range of credentials are linked to

Table 24. Use of credentials by disclosure of different types of personal data

		Biography information	Sensitive information	Security information
Use of credit cards and bank cards	Yes	.06	.01	.01
	No	-.63	-.08	-.12
Use of customer cards	Yes	.12	.05	.07
	No	-.17	-.07	-.09
Use of passport	Yes	.07		.06
	No	-.10		-.08
Use of government entitlement cards	Yes	.12		
	No	-.25		
Use of driving licence	Yes	.08		
	No	-.29		
Use of national identity cards/ residence permit	Yes			.04
	No			-.07

Source: QB4b by QB14.

Base: eCommerce users.

Notes: Results reported are means of disclosure of type of information [derived from factor analysis]. Only significant differences in the two-sided test of equality for column means are reported (p< 0.01: there is a 99% probability that differences reported are not due to chance).

the disclosure of what we called security-related information (mobile number, identity number and nationality). Overall, the structure of disclosure in eCommerce is dominated by privately-released credentials: credit cards and customer cards; government cards and identity cards only have a marginal role in the structure of disclosure. This should not be overstated. National identity cards are often the carrier of identity number and nationality that are disclosed by 18% and 35% of respondents, respectively. However, the use of ID cards is unrelated to disclosure of most information in eCommerce.

2.7.3 Risk

Risk perceptions in eCommerce are similar to risks perceived by other Internet users (including SNS users). However, there are also marked differences [all coefficients are reported in Table 25] which are briefly mentioned below:

- Those who are happier to disclose have a higher perception of identity theft risk than other people [r = .08, consistent with result on media awareness of identity theft risk, see Identification fact sheet].

- The minority of respondents who trust companies to protect their data perceive less risks of misuse of their data in eCommerce across the board [stealth use, unwanted offers, fraud]; the same does not work for institutions as data controllers – people who trust them and do not trust them do not have perceivably different attitudes to online data protection risks.

- Those using government-issued credentials are less likely to fear identity theft risk [r= -.12]; those using business-related credentials are more likely to fear identity theft risk [r = .06].

- People who fear risks of different nature are also more likely to take active steps to protect their personal identity, both online and offline.

- Comfort with online profiling mitigates the risk of unwanted commercial offers [r = .07] but not other risks to personal data.

- In the context of eCommerce, concern about unauthorised reuse of personal data is related to risks of identity theft and fraud, not with risks of unwanted commercial offers of stealth use of data [therefore substantive rather than procedural risks].

2.7.4. Responsibility

- People thinking that disclosure is unavoidable are more likely to think hey are responsible for protecting their own data, rather than companies. People who are happy to disclose think it is authorities who are responsible, rather than companies.

- Trust in companies as personal data controllers seem to reduce perceived authorities responsibility [r = -.13], and increase the perception of company and self responsibility [respectively r = .08 and r = .04].

- People considering authorities responsible have heightened concerns about observation [r = .10], reduced comfort about online profiling [r = -.10] and are more concerned about re-use of their data [r = .06]. In all these cases, people are also slightly more likely to think companies, rather than oneself, are responsible for correct handling of personal data [understandably, as there is little they can do].

- There is no relation between self responsibility and Internet protection behaviours and very little relation with identity protection behaviours in general. As found in previous surveys, even people feeling responsible do [as little] as the next person to protect their personal data once they have been disclosed. As it was noted above, this may be due to the lack of tools allowing people to take care, effectively if at all. But when tools are available, such as privacy notices, people do read them if they feel responsible [r = .10 for read and understand privacy statement, and negative relations for company and authorities responsibility].

- There is no relation between perceptions of responsibility in eCommerce and most other regulatory perceptions: possibility to delete one's data, portability of one's data and awareness/experience of identity theft and data loss.

2.7.5 Control

People who feel in control of their data trust companies and institutions to protect their data [r = .25 (!) and r = .12]; they are less concerned about observation [r = -.10], about re-use of their data [r = -.08] and more comfortable with online profiling [r = .18]; furthermore, they are far less likely to enjoy disclosing information [r = -.18].

In terms of behaviours, they do not shy away from disclosing [r = -.07], and do not engage any more frequently in online and offline identity protection behaviours. However, they are more likely to read and understand privacy statements [r = .13] and more likely to appreciate the possibility to move their data form one service provider to another [r = .10]. They do not have particular views on the possibility to delete their personal data.

Table 25. Correlations between eCommerce-related variables and other relevant variables

Variables			Disclosure				Risks			Responsibility			Control
	Measurement		3 Factors				4 Values			3 x 3-point scales			3-point scale
		Values	Biographic	Sensitive	Security	Stealth use	Unwanted offers	Identity theft	Fraud	Self	Company	Authorities	
Attitudes towards disclosure	2 Factors	Unavoidability	-.08	-.05	-.07		.04		-.04	.08	-.06		.06
		Propensity	.07	-.05	-.09	.04		.08	.04		-.07	.06	-.18
Trust	2 Factors	Trust in institutions	.08		.07		.08						.12
		Trust in companies	-.08		-.06	-.05	-.05		-.05	.04	.08	-.13	.25
Concern about observation	1 Factor			.04		.04					-.07	.10	-.10
Use of credentials in daily life	2 Factors	Business-related	.23	.04	.07		.04	.06	.06				-.07
		Government issued	.09				.06	-.12			-.04	.09	-.10
Identity protection behaviours	4 Factors	Do not disclose	.18	-.11		.07	.05	.06	.09				-.07
		Adjustment	.19		.09	.07	.12				.04		-.05
		Low-tech			-.04		-.05	.04		.05	-.05		
		Deception		.09	.05	-.06	.04			-.05			
Internet identity protection	9-points scale		.17	.05	.06		.06	.09	.08				
Awareness of identity theft and/or data loss	4 Values	Media awareness	.10		.06	.05		.09	.04				-.06
		Social awareness	-.08	.07	.07								
		Self-family experience		.11				.05	.04				
		No		-.05	-.05			-.07					.05
Comfort with online profiling	4-point scale		-.06				-.07			.04	.04	-.10	.18
Read privacy statements	3 Values	Read and understand	-.06	-.05					-.04	.10	-.06	-.05	.13
		Read no understand		.04								.04	-.04
		No read	.05			-.04				-.08	.07		-.09
Concern about reuse	4-point scale				-.05			.05	.04		-.07	.06	-.08
Possibility to delete personal data	1 Value	Whenever one wants	.13		.04	.05			.05				
Importance of personal data portability	4-point scale		-.04			.05			.05				.10

As the sample is large, only significant relations at $p < 0.001$ are reported [i.e. when there is a 99.9% probability that the relation reported is not due to chance].

Results reported are:

1. Pearson's correlation coefficient for pairs of factors and/or scales.

2. Point-biserial correlation for factors and/or scales crossed by values.

3. Phi for relations between values, when they can be considered as multiple categorical (e.g. colour: white, red, or green).

Note: Social information was excluded as it is marginal to the analysis, as it was noted in text.

3 FACT SHEET: Social Networking Sites

3.1 Question context

The questionnaire included several questions regarding disclosure and protection of personal data disclosed in the context of SNS, see Table 26:

Table 26. eID survey questions relevant to SNS

Question code	Shorthand	Formulation	Rationale
QB4a	Personal data disclosure	Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when registering, or simply when using these websites)?	To gauge the extent of disclosure of different types of personal data; this question follows on a previous questions asked of all respondents regarding what information they though was personal.
QB5a	Reasons why disclose	What are the most important reasons why you disclose such information on SNS and\ or sharing sites?	To assess the reasons why people disclose personal data in SNS, whether for leisure, to get better offers, to save time, etc.
QB6a	Control on information disclosed	How much control do you feel you have over the information you have disclosed on social networking sites and\ or sharing sites, e.g. the ability to change, delete or correct this information?	To determine the level of perceived control on the data disclosed in SNS. This is related both to the right of access to one's information and to the capacity of people to actually control their data once they have disclosed it.
QB7a	Risks related to disclosure	I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information on SNS and\ or sharing sites?	To explore the risks people associate with the disclosure of personal data in SNS. Several risks may be associated with disclosure, including risks to reputation, to persona safety, to data integrity and others.
QB8a	Information about consequences of disclosing personal information	Please tell me whether you agree or disagree with the following statement: SNS and\or sharing sites sufficiently inform their users about the possible consequences of disclosing personal information.	To assess user satisfaction with the information provided by SNS on the possible consequences of disclosure. Also to measure indirectly the awareness of these consequences.
QB9a1 & QB9a2	Responsibility to protect	Who do you think should make sure that your information is collected, stored and exchanged safely on social networking sites and\ or sharing sites? Firstly?	To help determine who people think is responsible for the protection of personal data once it's been disclosed.
QB10a	Privacy settings	Have you ever tried to change the privacy settings of your personal profile from the default settings on a social networking site and\ or sharing site?	To identify people's behaviours regarding privacy settings.
QB11a	Privacy settings difficulties	How easy or difficult did you find it to change the privacy settings of your personal profile?	To identify people's perception of ease regarding privacy settings changes.
QB12a	Privacy settings	Why did you not try to change these privacy settings?	To understand the reasons why people do not try to change their privacy settings.

For details regarding the methodology used in the survey, please refer to the main report. Some of the question in the survey we asked both of social networking site users and of people using online sharing sites. In this fact sheet, we examine the responses – behaviours, attitudes – of social networking site users [henceforth: SNS users].

3.2 Legal context

Taking into account that Social Networking Sites are not currently regulated, the main legal instruments and policy initiatives with regard to SNS are the following:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Specifically the survey asks questions related to the information received on the collection of personal data and on the type of information disclosed on SNS (such as health information and/or information regarding third parties), useful to understand the effectiveness on Internet of some specific Data protection restrictions. In addition, the survey asks questions relevant to data loss and data breach notification,[22] which may assist the number of people that are happy to disclose personal data, that are less likely to minimise data and that rarely use software measures to protect their data. On the right balance to be stroke between enhanced control and self-protection and enforcement of actor-based rules. And on the relation between online identity management and people's regulatory preferences regarding data protection. Questions regarding the effective use of data subject's right of access to data in order to update it or delete it are also relevant for the current discussion on the so-called right to be forgotten and for a possible revision on how should such right be obtained from the controller.[23]

- Directive 1999/93/EC on a Community framework for electronic signatures, and the proposal for a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems [DAE Key Action 16]. The survey does not look specifically at the use of eSignature, as individual users' uptake is low across Member States; however, it looks at use of credentials and at strategies for protecting one's identity and transactions online, including in eCommerce [in MS, cross-border], eGov and SNS (for example asking what measures are adopted to protect one's own identity). One of the main reasons for disclosure when using SNS is to access the service and to connect with others. This may assist the framing of the eSignature debate in wider terms (towards reaching a more secure *Digital Single Market*).

- Directive 2006/123/EC on services in the internal market. The survey looks at the relation between identification mechanisms, online self protection and the fruition of eServices such as eCommerce, SNS and home banking.

- Directive 2002/58/EC ("e-privacy") concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), namely the need for users to 'opt in' – that is consent following clear and comprehensive information. The survey asks questions related

22 "… the possible modalities for the introduction in the general legal framework of a general personal data breach notification, including the addressees of such notifications and the threshold beyond which the obligation to notify should apply" (in "A comprehensive strategy on data protection in the European Union", EC 2010).

23 E.g. through privacy-friendly default setting, given the fact that, as stressed by the EDPS in its Opinion of 18th March 20101 on promoting Trust in the Information Society by fostering data protection and privacy, users are often unaware of their acting as data controllers of other people's data.

to users' awareness of possible accessibility of their data by third parties, information received on privacy settings as well as about the use of tools to limit unwanted email or cookies; questions regarding users' concerns about further uses of data than original ones, and about profiling (the majority of the interviewers are uncomfortable about that) are important for the preannounced review of the Directive. As stressed by EDPS,[24] "social network […] should also require user's affirmative consent before any profile becomes accessible to other third parties, and restricted access profiles should not be discoverable by internal search engines". Questions about *the reasons for deleting personal data, importance of data portability across providers and platforms and incidence of changing privacy settings on social networking sites* are also relevant for the future comprehensive framework on DP focused on enhancing users' control over their data (including the strengthening of the right to be forgotten and data portability).[25]

- Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. The survey asks several questions relevant to understand the awareness of users about the conditions of data collection and about the further uses of data when joining SNS; questions on *perception of risks* by the users and on *reasons for deleting data* are also relevant for the current debate of the Directive.

- Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. This Directive introduced in particular the obligation of data breach notification, though, up to date, applies only to providers of publicly available electronic communication services. The concerns (about data over-disclosure, loss or theft) emerging from the questions asked in the survey give evidences on the need for a comprehensive framework on DP, extending the security obligations across sectors.

- The Consumer Rights Directive, still at proposal stage, which should replace and merge 4 existing consumers rights Directives (Sale of consumer goods and guarantees (99/44/EC); Unfair contract terms (93/13/EC); Distance selling (97/7/EC); Doorstep selling (85/577/EC) and the revision of the EU data protection regulatory framework with a view to enhancing individuals' confidence and strengthening their rights [DAE Key action 4]. The survey examines issues of internet skills in relation to identity protection online and offline, and awareness of identity theft and data breach.

- Considering the use of SNS and the risks perceived by users as emerging from the survey, applicable norms are also those of the Directive 2001/95 on general product safety (art 2 defines a product as 'any product - including in the context of providing a service – which is intended for consumer or likely").[26]

24 EDPS, European Data Protection Supervisor, Opinion on promoting Trust…cit supra note.

25 Communication from the Commission A Comprehensive approach on personal data protection in the European Union, COM (2010) 609, 2.1.

26 See: Whereas 7: "This Directive should apply to products irrespective of the selling techniques, including distance and electronic selling" and Whereas 9: "This Directive does not cover services, but in order to secure the attainment of the protection objectives in question, its provisions should also apply to products that are supplied or made available to consumers in the context of service provision for use by them".

- The proposal for a Directive of the European Parliament and of the Council on combating sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM/2010/0094 final - COD 2010/0064,[27] (Art 21 of the proposal is on Blocking access to websites containing child pornography) . The survey asks about the perceived risks associated with the use of SNS (among which emerge the perception *of personal safety being at risk, of own information being shared with third parties without consent, of personal data being used in different contexts and of own identity being at risk of theft online*), that, though not expressly mentioned, can be risks related to child pornography (the majority of 'digital natives' use Internet and SNS).[28]

- Self-regulation of social networking sites has been encouraged by the European Commission, as part of its Safer Internet Plus Programme; all those who create new interactive tools are encouraged to adopt rules and principles themselves (self-regulation). This is the case of the so-called Safer Social Networking Principles (ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf), which have been developed by SNS providers in consultation with the European Commission, to provide good practice recommendations for the providers of social networking and other user interactive sites, enhancing the safety of children and young people using their services. Questions posed by the survey regarding the disclosure of personal data and the control on information disclosed, and especially the questions concerning risks related to disclosure and responsibility attribution for the collection, storage and the safe exchange of information on SNS sites, are of direct relevance to the above mentioned SNS principles. Namely to the one that enables and encourages users to employ a safe approach to personal information and privacy. Questions regarding the use of tools to limit unwanted email or cookies, as well as questions regarding users' concerns about the further uses of data than the original ones, and about profiling are relevant for the implementation of the principle that empowers users through tools and technology. The data collected in this survey regarding the attitudes and the behaviours of young people using SNS may prove to be important for the further development and implementation of SNS legal principles at the EU level.

3.3 SNS users: socio demographic characteristics / Internet activities

More than half of Internet users (52%), therefore about a third of all Europeans, use SNS. This is less than the number of Internet users that purchase goods or services online (60%). However, several differences appear in terms of socio demographic characteristics, in particular regarding age; education, occupation, and Internet use [see Figure 5]. Specifically, SNS users are more likely to be younger, typically female, well educated, they are heavier Internet users and are still studying or are unemployed. In contrast, eCommerce users are older (25-55), typically male, better educated, heavy Internet users, in management positions or self-employed and generally more affluent.

To confirm the complementarities of Internet activities, means of variables and their correlation were checked. More than half of SNS users also utilised websites to share pictures, videos, movies, etc, (68%); instant messaging, chat

27 OJ L 13, 20.1.2004, p. 14.

28 The objectives – as stated in the same proposal – "are consistent with the Safer Internet Programme set up to promote safer use of the internet and new online technologies, particularly for children, and to fight against illegal content […] and also with the new EU Youth Strategy (Council Resolution 27 November 2009), which targets children and young people within the age range 13-20, and anchors European youth policy cooperation firmly in the international system of human rights".

Figure 5. Socio-economic profile of SNS users

Use a social networking site

	Yes	No	DK
EU27	52%	48%	-
Sex			
Male	50%	50%	-
Female	54%	46%	-
Age			
15-24	84%	16%	-
25-39	62%	38%	-
40-54	36%	64%	-
55 +	22%	77%	1%
Education (End of)			
15-	35%	64%	1%
16-19	48%	52%	-
20+	48%	51%	1%
Still studying	85%	15%	-
Household composition			
1	50%	50%	-
2	43%	56%	1%
3	57%	43%	-
4+	58%	42%	-

Household composition			
1	50%	50%	-
2	43%	56%	1%
3	57%	43%	-
4+	58%	42%	-
Respondent occupation scale			
Self-employed	44%	56%	-
Managers	47%	53%	-
Other white collars	52%	47%	1%
Manual workers	51%	49%	-
House persons	51%	49%	-
Unemployed	64%	35%	1%
Retired	22%	77%	1%
Students	85%	15%	-
Use of the Internet			
Everyday	60%	40%	-
Often/ Sometimes	30%	69%	1%
Never	-	-	-
Difficulties paying bills			
Most of the time	62%	38%	-
From time to time	57%	43%	-
Almost never	48%	51%	1%

Source: QB1a.2.
Base: Internet users.

websites (57%) and have purchased goods or services online (57%). Other advanced Internet activities, such as use of online software, making or receiving phone calls or video calls over the Internet and use of peer-to-peer software to exchange music are reported by a third of European SNS users. Therefore, SNS users are as 'green' as generally believed; but they are also able to harness the Internet to a greater extent than previously known.

Factor analysis was used to assess item correlations and identify common relationships between similar items, allowing the items to be categorized into themes or factors.[29] This analysis yields three statistically significant and conceptually meaningful factors [see Table 27].

The first factor includes Internet activities that are related with the use of SNS: use of sharing site; instant messaging and phone calls or video calls over the Internet. Therefore, it is labelled as representing "Social" Internet activities. The second factor Internet activities included home banking; purchase goods or services online and submit tax declaration or use other online government services, and may be interpreted as "Transactional" Internet activities. Finally, the third factor includes activities such as designing or maintaining a website (not just a blog); install plug-ins in your browser to extend its capability; keep a blog (also known as web-log); use online software and use peer-to-peer software or sites to exchange movies, music. Unlike the previous two factors, that are largely conducted online, these activities are all related with the utilisation of software, online and offline. Thus, this factor is labelled as "Software", representing an advanced use of the Internet.

29 An analysis of the correlation matrix (KMO and Bartlett's test of sphericity) was carried out to check that the correlation matrixes were factorable. Data reductions were undertaken by principal components analysis using the Varimax option to identify possible underlying dimensions.

Table 27. Factor analysis of Internet activities

	Factor 1. Social activities	Factor 2. Transactions	Factor 3. Software activities
Use a social networking site	.78		
Online sharing sites	.75		
Instant messaging, chat websites	.71		
VoIP	.41		
Home banking		.79	
Purchase goods or services online		.68	
eGovernment		.68	
Design or maintain a website (not just a blog)			.69
Browser plug-ins			.59
Keep a blog (also known as web-log)			.58
Use online software			.50
Use peer-to-peer software or sites	.42		.46
Auto values	2.87	1.67	1.08
% Variance explained	24	14	9

Source: QB1a and QB1b.

Base: Internet users.

Notes: Rotated components matrix: factor analysis by main components; Rotation: Varimax with Kaiser-Meyer-Olkin 0.781; Bartlett's test of sphericity p=0.000; Convergence in 4 iterations; Minimum eigenvalue 1; Values below .04 are omitted.

Finally, we sketch a profile of SNS users, based on their attitudes, behaviours and regulatory preferences regarding personal identity data disclosure, vis-à-vis other Internet users who do not use SNS, and the general public [Table 28, Table 29, Table 30]. This helps contextualise the analysis of actual disclosure taking place in SNS, which comes later in this fact sheet.

Attitudes of SNS users [Table 28]:

- **SNS users care as much about their sensitive information [medical, financial, etc.] as the next Internet user, but they care much less about their social information.** SNS users consider their social information [friends, activities, etc.] more personal than offline respondents do, and much less than the average Internet user. But they consider their sensitive information [financial, medical fingerprints] as personal as Internet users do [and much more than the general public]. This may give indication on the appropriate level of co-regulation of industrial practice in the field of SNS: sensitive information needs outright protection online, while social information may need ad-hoc safeguards, as SNS users are less cautious [more on this later in the sheet].

- **SNS users are more realistic than the average Internet user regarding the need to disclose, but they are less virtuous.** SNS users have stronger feelings about disclosure than Internet users and non-users; on the one hand, they think that disclosure is unavoidable in today's' life, much more so than Internet users and the general public [also see Table 35]. But on the other hand they do not seem to resist the push to disclose: they are far happier to disclose their personal information than Internet users [strikingly, Internet users are even less happy to disclose personal data than people offline].

Table 28. Attitudes of Internet non-users, Internet users and SNS users

		Measurement	No Internet	Internet -SNS use	Internet +SNS use
Attitudes	Biography information is personal	Factor score	.07	.05	**.12***
	Social information is personal	Factor score	-.15*	.39*	.17*
	Sensitive information is personal	Factor score	-.34*	.06	.07
	Disclosure is unavoidable	Factor score	-.20*	-.03*	**.17***
	…[Internet users only with specific questions]	Factor score	---	-.13	**.11**
	Disclose happily	Factor score	-.06	-.10	**.13***
	…[Internet users only with specific questions]	Factor score	---	-.16	**.14**
	Concern regarding observation on the Internet	1-4 scale	3.3	2.7	2.5
	Concern regarding observation in a public space	1-4 scale	2.3	2.3	2.2
	Concern regarding observation in a private space	1-4 scale	2.4	2.5	2.4
	Concern regarding observation via mobile phone/ mobile Internet	1-4 scale	2.7	2.7	2.6
	Concern regarding observation via payment cards	1-4 scale	2.8	2.8	2.7
	Concern regarding observation via store or loyalty cards	1-4 scale	2.6	2.6	2.3
	Comfort with online profiling	1-4 scale	---	2.12*	**2.45***
	Concern about stealth re-use of personal data for other purpose than original	1-4 scale	2.91*	3.01*	2.86*
	Trust in institutions as personal data handlers	Factor score	-.19*	-.01*	**.13***
	Trust in companies as personal data handlers	Factor score	-.25*	-.08*	**.22***

Source: qb1a_2_RCb, qb1_RC_#_all, FAC1_2 qb2, FAC2_2 qb2, FAC3_2 qb2, FAC1 qb3 [all], FAC2 qb3 [all], qb13_1, qb13_2, qb13_3, qb13_4, qb13_5, qb13_6, qb_13_FAC1_all, FAC2_4, FAC1_4, qb16_#_total, qb16_factors, qb17_RC, qb21_RC, FAC1_7, FAC2_7, qb22_RC, qb26_RC, qb28.1, qb29_RC, qb31_RC , qb32_RC.

Base: EU27 and Internet users [where the "---" mark is used].

*Notes: * means that differences are significant at $p < 0.001$ [i.e. when there is a 99% probability that the difference reported is not due to chance].*

Results and figures should be interpreted 'horizontally' only across dividing lines, as the scale of measurement varies between variables.

- SNS users are as concerned as others about being 'observed' in a range of situations online and offline. If anything, they are slightly less wary of observation, possibly due to their younger age. Interestingly, **SNS users are less concerned in relation to online observation, and also significantly more comfortable with online profiling in exchange for free services.** This may be due to SNS users' higher level of trust in institutions and companies as controllers of their personal data than otherwise internet users.

Behaviours of SNS users [Table 29]:

- SNS users are less likely than Internet users to use private credentials [credit cards, driving license, etc]; this may be due to younger age. They are also less likely than any other group to use government-related credentials. What this means for online identification and authentication is explored in greater depth in the Identification fact sheet.

- SNS users are more likely than Internet users to report to have been informed about data collection conditions when disclosing personal data to access an online service; however, they also felt they were required to provide more personal information than necessary to access the online service.

- SNS users use a slightly wider range of strategies to protect their personal data online than the average Internet user. What is more interesting is that they are less likely to use traditional security measure [not revealing user names etc.] and 'offline' protection [use cash]; and they are more likely to use software-based responses

Table 29. Behaviours of Internet non-users, Internet users and SNS users

		Measurement	No Internet	Internet -SNS use	Internet +SNS use
Behaviours	Use of credentials in daily life - Private	Factor score	-.52*	.36*	.18*
	Use of credentials in daily life - Government	Factor score	.16*	-.02*	-.15*
	Informed about data collection conditions when disclosing to access a service	1-4 scale	---	2.59*	2.87*
	Required to provide more personal information than necessary for online services	1-4 scale	---	2.04*	2.29*
	Tot number of online identity protection measures taken	1-9 scale	---	2.04*	2.60*
	Reactive identity protection	Factor score	---	-.12*	.11*
	Proactive identity protection	Factor score	---	-.15*	.14*
	Withholding identity protection	Factor score	---	.08*	-.07*
	Low-tech identity protection	Factor score	---	.07*	-.07*

Source: qb1a_2_RCb, qb1_RC_#_all, FAC1_2 qb2, FAC2_2 qb2, FAC3_2 qb2, FAC1 qb3 [all], FAC2 qb3 [all], qb13_1, qb13_2, qb13_3, qb13_4, qb13_5, qb13_6, qb_13_FAC1_all, FAC2_4, FAC1_4, qb16_#_total, qb16_factors, qb17_RC, qb21_RC, FAC1_7, FAC2_7, qb22_RC, qb26_RC, qb28.1, qb29_RC, qb31_RC , qb32_RC.

*Notes: * means that differences are significant at p < 0.001 [i.e. when there is a 99% probability that the difference reported is not due to chance].*

Results and figures should be interpreted 'horizontally' only across dividing lines, as the scale of measurement varies between variables.

Table 30. Regulatory preferences of Internet non-users, Internet users and SNS users

		Measurement	No Internet	Internet -SNS use	Internet +SNS use
Regulation	Possibility to move personal data between service providers	1-4 scale	---	2.95*	3.04*
	Importance of having same data protection right across Europe	1-4 scale	3.34*	3.54	3.56
	Desire to be informed by controller whenever personal data is lost/stolen	% agree	87%	92%	93%
	Possibility to delete personal data held whenever you decide to delete it	% agree	---	73%	77%

Source: qb1a_2_RCb, qb1_RC_#_all, FAC1_2 qb2, FAC2_2 qb2, FAC3_2 qb2, FAC1 qb3 [all], FAC2 qb3 [all], qb13_1, qb13_2, qb13_3, qb13_4, qb13_5, qb13_6, qb_13_FAC1_all, FAC2_4, FAC1_4, qb16_#_total, qb16_factors, qb17_RC, qb21_RC, FAC1_7, FAC2_7, qb22_RC, qb26_RC, qb28.1, qb29_RC, qb31_RC , qb32_RC.

Base: EU27 and Internet users [where the "---" mark is used].

*Notes: * means that differences are significant at p < 0.001 [i.e. when there is a 99% probability that the difference reported is not due to chance].*

Results and figures should be interpreted 'horizontally' only across dividing lines, as the scale of measurement varies between variables.

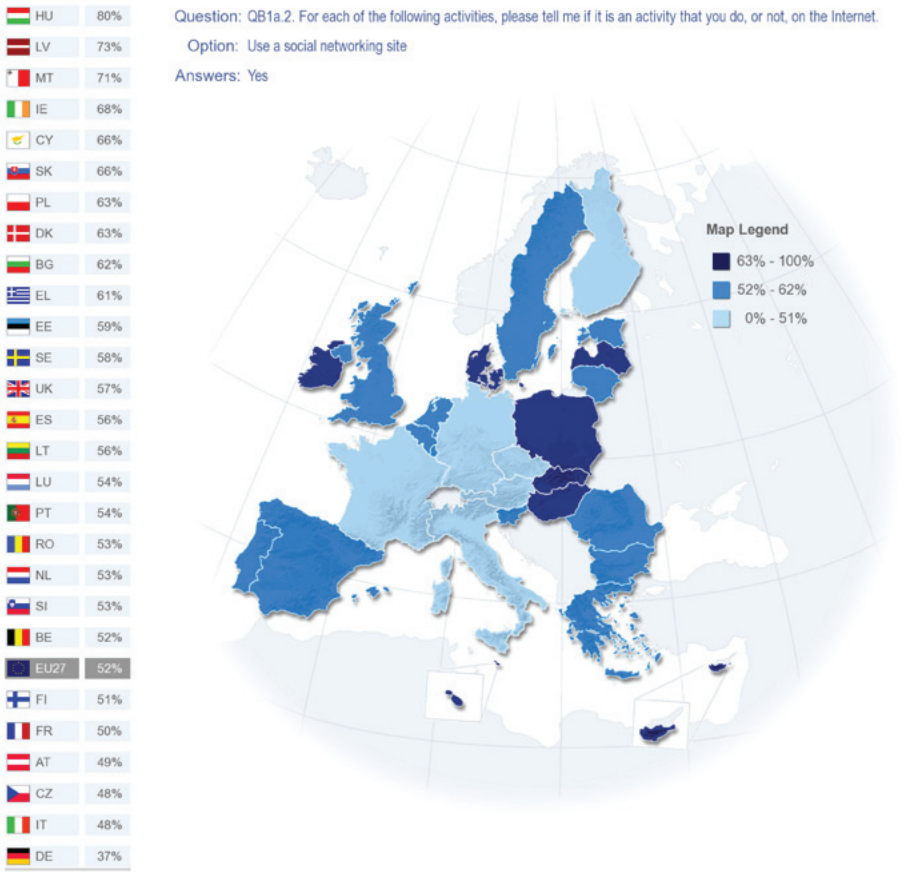
[e.g. anti-spam], and active information management strategies [e.g. using search engines to maintain awareness]. This is a clear case of horses for courses, and relatively sophisticated focusing of protection behaviour on a perceived threat.

Strikingly, SNS users have similar regulatory preferences to Internet users concerning the protection of personal data [Table 30], both quite more vigorous than non Internet users; therefore, technology-specific and local regulatory solutions [control tools, breach notification, portability, deletion on demand] may be more suitable to tackle issues of disclosure in SNS environments than general regulation [however important this remains]. SNS users are slightly more in favour of such local solution that the average internet user.

3.4 National differences in SNS use

Beyond social characteristics, we found that there are significant national differences in the uptake of SNS users in Europe [Figure 6]. Social networking sites are used most often in Hungary (80%), Latvia (73%), Malta (71%), Ireland (68%), Cyprus, Slovakia (both 66%), Poland and Denmark (both 63%), and least in Germany (37%).

Figure 6. Distribution of SNS users in EU27



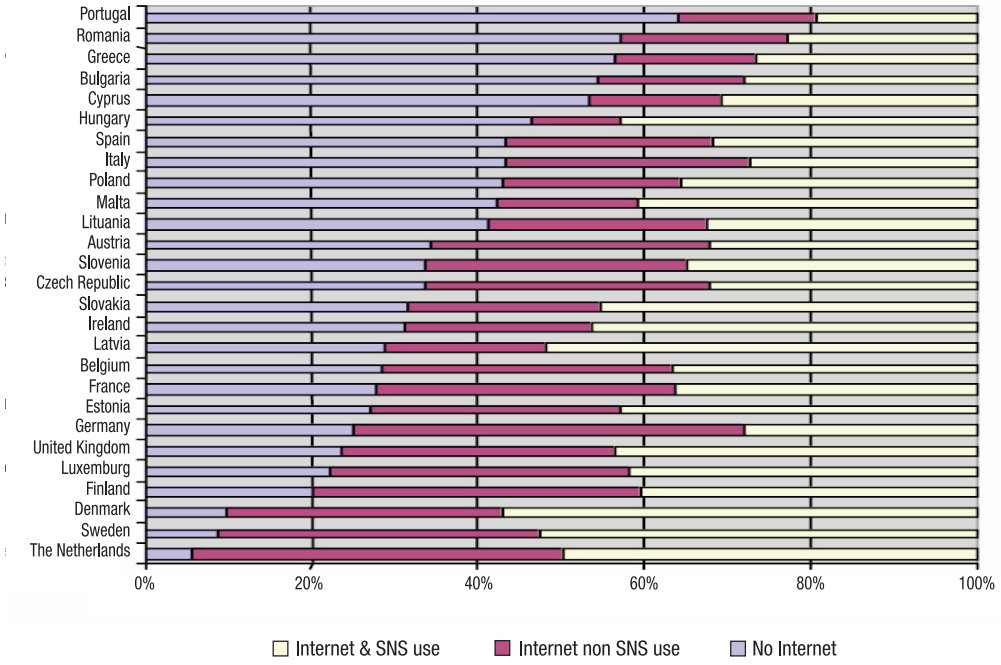
Base: Internet users (66% of total sample).

There is a clear correlation between the rate of Internet use in a country, and the proportion of people using SNS online: the more the internet is widespread, the more Internet users also use SNS. This is not intuitive: one may think that, given internet access, people [young people, mainly] in different countries will have the same propensity to use SNS [Figure 7]. It is evident that the proportion of people using SNS [yellow bar] increases vs. people not using SNS, [red bar], as Internet access increases [blue bar]. Indeed, the correlation is strong [r = 0.61] between SNS and Internet use across EU27 [Figure 8]. This apparent idiosyncrasy is due to the socio-demographics underpinning internet uptake [affluence, education, age], which also strongly influence SNS use.[30]

Nevertheless, in the case of SNS use unlike in the case of eCommerce, age plays a key role at national level. We have identified four different

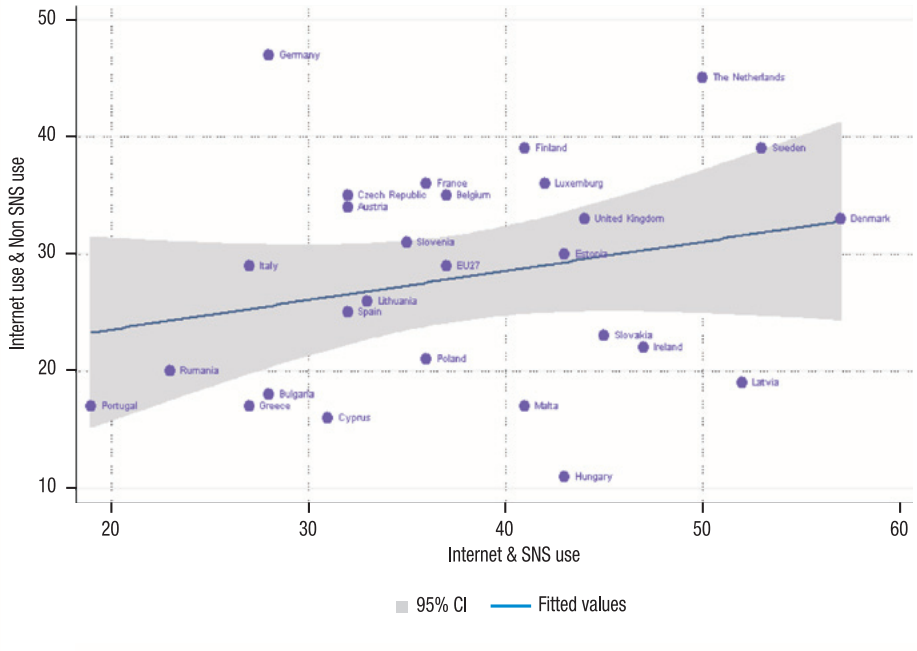
30 See socio-demographic characteristics of SNS users as presented in [Figure 5].

Figure 7. Internet & non SNS use, Internet & SNS use and non Internet use EU27



Base: Total population.

Figure 8. Linear Internet and non SNS use and Internet and SNS use EU27



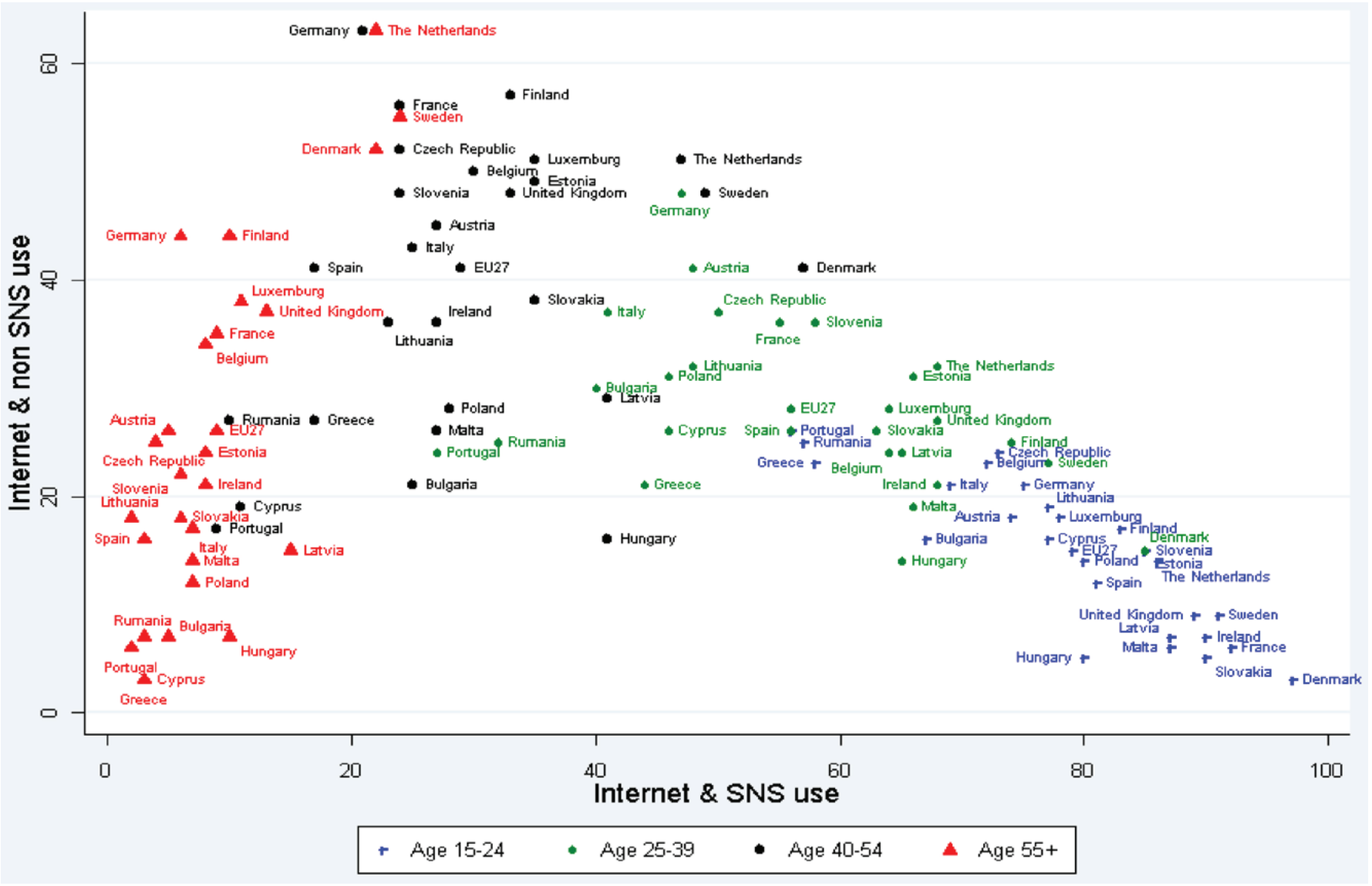
Source	SS	df	MS
Model	3676.31748	1	3676.31748
Residual	2179.31215	25	87.1724859
Total	5855.62963	26	225.216524

Number of obs = 27
F(1, 25) = 42.17
Prob > F = 0.0000
R-squared = 0.6278
Adj R-squared = 0.6129
Root MSE = 9.3366

internetuse	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
internetsn~e	1.238003	.1906359	6.49	0.000	.8453805	1.630625
_cons	18.80242	7.381475	2.55	0.017	3.599989	34.00485

Base: Total population.

Figure 9. Internet and non SNS use and Internet and SNS use EU27 by age



Personal data disclosure in SNS.

trends related with four different age brackets in relation to Internet vs. SNS use [Figure 9]. In other words, younger people in most EU countries use the Internet very little outside SNS, almost necessarily for people aged 15-24 years old, but also strongly for people aged between 25-39 years of age. The situation is very different for people aged 55+: SNS use is largely rigid on Internet use, which means that older people who use SNS do it for reasons different than other internet use; alternatively, that SNS is not quite built into Internet use overall. For these two groups, age and Internet dynamics matter more than country in predicting SNS use. For the other group [40-54], there is a positive relation between the two, as was described above: in countries where Internet use is high, people tend to use more SNS as well.

This dispels the idea that SNS may be an 'easier' entry point for all into other Internet activities; SNS rather tends to be unrelated to Internet use for older groups [use is more similar across countries regardless of Internet penetration]; it tends to build on and reinforce the same factors predicting Internet uptake for middle-age Europeans; but it tends to be an entry point and substitute other Internet uses for younger people. For young professionals, specifically, country of residence counts as much as age in predicting uptake of SNS. In fact, it also remains true that some countries, across age brackets and Internet usage, host more SNS users as a percentage of Internet users, and less respectively: Nordic countries on the one hand, Portugal, Rumania and Greece on the other hand.

3.5 Personal data disclosure in SNS

SNS users were then asked about the types of information they disclosed when they registered or simply used these website.[31]

Table 31. Personal information disclosed in SNS

	% of SNS users
Name	84%
Photos	57%
Nationality	51%
Activities	43%
Who friends are	43%
Address	41%
Preferences	36%
Mobile Number	23%
Work history	19%
Website visited	15%
National identity Number	13%
Financial	9%
Medical information	5%
Fingerprints	4%
None	4%
Other	1%
D.K.	1%

Source: QB4a.

Base: SNS users.

31 Question QB4a: Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?

Table 32. Factor analysis of personal information disclosed in SNS

	Factor 1. Social information	Factor 2. Sensitive information	Factor 3. Traditional identifiers
Who friends are	.76		
Photos	.75		
Activities	.75		
Preferences	.73		
Websites visited	.46		
Work history			
Fingerprints		.76	
Medical information		.75	
Financial information		.69	
National Identity number		.61	.33
Address			.81
Mobile number			.67
Name	.31	-.35	.58
Nationality	.42		.51
Eigenvalue	3.10	2.43	1.56
% Variance explained	22.2	17.3	11.1

Source: QB4a.

Base: SNS users.

Notes: Rotated components matrix; Sampling method: factor analysis by main components;

Rotation method: Varimax with Kaiser-Meyer-Olkin 0. 786; Bartlett's test of sphericity p=0.000; Convergence in 4 iterations; Minimum eigenvalue 1; Values below 0.3 are omitted.

Most SNS users revealed their name (84%) and more than half revealed photos (57%) and nationality (51%). Furthermore, activities and friends were disclosed by 43% of SNS users while address is disclosed by 41%. Financial information, medical information and fingerprints are all disclosed by less than 10% of SNS users.

To confirm the several internal complementarities of the personal information disclosed in SNS, factor analysis was carried out (see Table 32). This analysis identified three statistically significant and conceptually separate types of information disclosed. The first type includes who friends are, photos, activities, preferences and websites visited. Therefore, it is labelled "Social information". The second factor includes work history, fingerprints, medical information, financial information and national identity number. These types of information appears to be biographical in nature, and are disclosed by far fewer respondents than other information; we thus named it "Sensitive information". Finally, the third factor includes address, mobile number, name and nationality; thus, this factor is labelled as "Traditional identifiers". This may be a slight misnomer, as 'mobile phone' is included in the factor. Alongside email disclosure, which is mandated by almost every SNS operator, these are items that people 'have to' disclose if they want a profile set up on SNS. The place of mobiles in the structure of identification / authentication is discussed in greater depth in the fact sheet on eCommerce.

In terms of socio-economic status, age appears to play the most important role in the disclosure of many of the items reported. SNS users who are still studying are more likely to disclose more items than less educated individuals [up to 15 years old regarding age left education], especially of social nature [Table 33]. Students, single people with mobile phones also tend to disclose more information across the board than average SNS users; strangely, the difference is greater for mobile phone users concerning disclosure of biographical information such as age, address and nationality.

We then examined whether people disclosed more or less of different types of information in different countries. To provide a more structured view on the results, we looked at country differences in the provision of 'clusters' of personal data, as they were determined using factor analysis: social information, sensitive information and traditional identifiers [Table 34].[32] Overall, we

32 A breakdown for individual items by every single country is reported in Section 3.9.

Table 33. Personal data disclosure in SNS by socio-economic status

		Financial	Work history	National identity number	Name	Address	Nationality	Activities	Preferences	Photos	Friends	Web site visited	Mobile number
	EU27	11%	17%	16%	82%	42%	50%	40%	32%	52%	38%	17%	26%
Age [brackets]	15-24	7%	16%	11%	87%		55%	51%	44%	68%	52%	20%	
	25-39		23%			39%	53%	44%	38%	58%			
	40-54	12%				44%	45%	35%	26%	44%	32%	12%	
	55+		13%		75%	46%	40%	22%	19%	33%	27%	10%	
Terminal education age	15-							31%	27%	25%			
	16-19									50%			
	20+		26%									14%	
	Still Studying	7%	14%	10%			55%	52%	44%	69%	55%	20%	
Occupation	Self-employed	13%		16%			47%	38%	30%		35%		
	Managers		28%								40%	13%	
	Other white collars		22%									13%	
	Manual workers										41%	14%	
	House person					35%		38%					17%
	Unemployed				86%	45%							
	Retired		11%		76%		42%			35%	29%	12%	19%
	Students	7%	14%	11%	86%	39%	55%	28%	25%	69%	55%	20%	
Personal mobile phone	No		8%		60%	23%	36%						13%
	Yes		20%		84%	41%	51%						24%

Source: QB4a.

Base: SNS users.

Notes: Only significant difference at p < 0.001 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

We have highlighted in green the values most different from the EU27 mean.

Table 34. Information disclosed in SNS by country

	Social information	Sensitive information	Traditional identifiers
Belgium	0.1	0.02	0.07
Denmark	0.2	-0.01	0.43
Greece	-0.2	0.03	-0.09
Spain	0.01	0.39	0.1
Finland	0	-0.1	0.23
France	0.04	-0.16	-0.04
Ireland	0.21	0.03	0.17
Italy	0.06	0.23	-0.3
Luxemburg	0.39	-0.15	-0.1
The Netherlands	0.14	-0.14	-0.01
Austria	0.28	0.34	0.32
Portugal	-0.18	0.28	-0.21
Sweden	0.23	0.13	0.69
United Kingdom	0.16	-0.21	-0.35
Germany	-0.07	-0.1	0.15
Bulgaria	0.02	-0.06	-0.21
Cyprus	-0.06	-0.12	0.16
Czech Republic	-0.18	0.06	0.25
Estonia	0.02	0.39	0.3
Hungary	-0.12	0.19	0.1
Latvia	-0.17	0.13	0.38
Lithuania	-0.06	-0.14	-0.17
Malta	0.3	-0.07	0.16
Poland	-0.46	-0.17	0.26
Romania	-0.13	0.32	-0.15
Slovakia	-0.03	0.05	0.31
Slovenia	-0.08	-0.11	0.22
EU27	0.02	0.03	0.12

Source: QB4a.
Base: SNS users.

found no discernible regional patterns concerning overall disclosure. In terms of social information, people disclose much less in Poland [but in general also in other east European countries], and much more in Sweden, UK and Luxembourg and Austria. Regarding sensitive information, people in Spain, Austria, Estonia and Romania disclose more, while people in the UK, France and Poland disclose less. When we turn to traditional identifiers, people in Sweden, Denmark and Latvia disclose more [possibly due to higher mobile phone number disclosure or as a result of their increased use of eGov services], while people in the UK and Italy disclose less [possibly because in the UK they use less traditional identifiers and in Italy since e-services are not as diffused]. These fragmented results, apart from national exceptions, may mean that SNS are still very national, as people do disclose different types of information on language based-sites [for instance Tuenti {www.tuenti.com} in Spain]; results may also be due to country specific culture and regulation which was not tapped in the survey.[33]

3.5.1 Need to disclose in SNS

Turning to perceptions of the necessity of disclosing personal information, respondents were asked seven statements addressing this

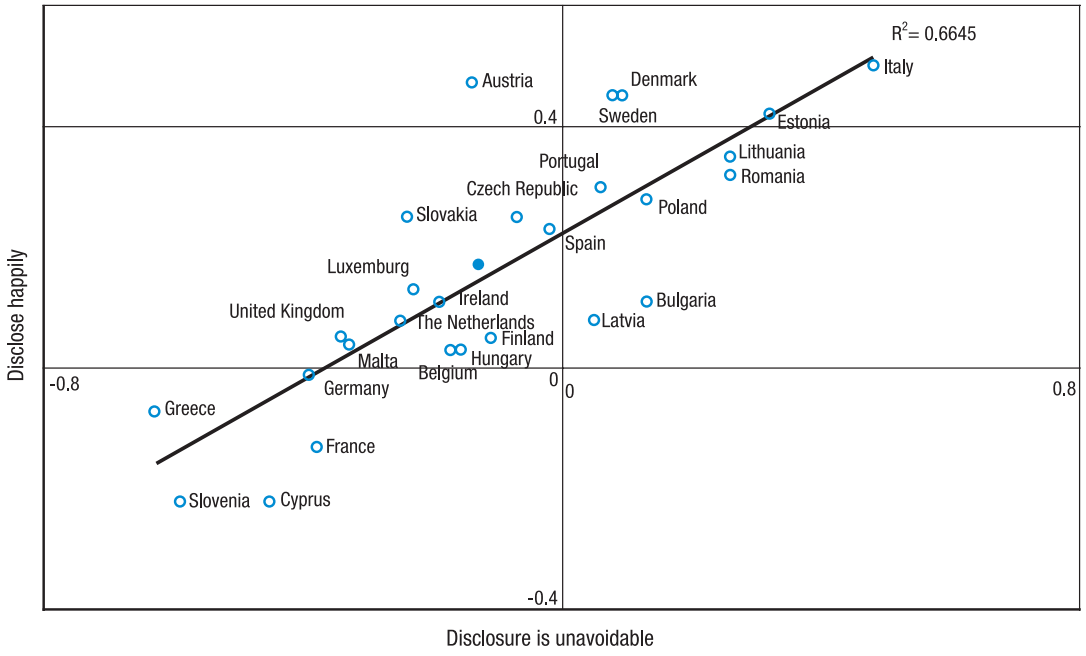
33 This, in turn, hints at the importance of conducting supply-side analysis of the type of information required / elicited by different SNS operators across EU27.

Table 35. Perceptions of the necessity of disclosing personal information by SNS use

	Totally Agree	
	% of non SNS user	% of SNS user
Nowadays you need to log into several systems using several usernames and passwords	79%*	86%*
Disclosing personal information is an increasing part of modern life	78%*	84%*
The (NATIONALITY) Government asks you for more and more personal information	69%*	72%*
There is no alternative than to disclose personal information if one wants to obtain products or services	64%*	72%*
You feel obliged to disclose personal information on the Internet	33%*	44%*
You don't mind disclosing personal information in return for free services online (e.g. free email address)	32%*	44%*
Disclosing personal information is not a big issue for you	30%*	39%*

Base: EU27.
Source: QB5b.
*Note: *p<0.001 are reported.*

Figure 10. Attitudes to disclosure in EU27 countries



Base: SNS users.
Source: QB5b.

issue [Table 35].[34] Individuals who use SNS are more likely than non SNS users to agree that 'disclosing personal information is an increasing part of modern life' (84%). SNS users feel more of an obligation to disclose than non SNS users (44%). They have a stronger perception that the government asks for increasingly more personal information and that there is no alternative than to disclose personal information if one wants to obtain products or services (both at 72%). However, SNS users are more likely not to mind disclosing personal information in return for free services online (e.g. free email address) (44%).

We then looked at country level, to see whether there are national differences in the relation between the feeling of unavoidability

34 Qb5b. What are the most important reasons why you disclose such information on social networking sites?

to disclose, and the desire to disclose.[35] At country level, the situation is different and interestingly, pointing at context effects on the relationship [Figure 10]. In some countries, SNS users are slightly more likely to disclose happily [Italy, Estonia], and to think that disclosure is unavoidable. Conversely, in other countries [Greece, Cyprus, Slovenia], people are less likely to be happy to disclose their personal data; they also think that disclosure could be avoided. Unavoidability of disclosure is also related to the benefit of the service obtained through data disclosure.

3.5.2 Disclosure in SNS: what is personal and reasons for disclosure

We then crossed disclosure of data with the perception that this data is actually personal. This tells us whether people who disclose personal data consider it as such.[36] Overall, there is no apparent relation between considering one's data personal and disclosing them on SNS. So even if people consider information personal, still they disclose it. If anything, people disclose information slightly more if they consider it personal; this may be because people attribute importance ex-post facto having disclosed the information. Of course, this may be due to the fact that people need to disclose social information if they want to socialise online. Indeed, the most important reasons for disclosing personal information when using SNS are to access the services (61%) followed by connect with others (54%).[37] Both reasons are related with a functional requirement and with core socialisation – the main aim of SNS. Other reasons, such as 'for fun' (23%), to get a service for free and to obtain a customised service (both at 17%) point out that 'functional' aspects are also considered by SNS users to disclose information, albeit to a much lesser extent.

Furthermore, there is a clear link between information disclosed and reason for disclosing information in relation 'to connect with others' and 'fun' [Table 37]. Both reasons are related to disclosure of social information on SNS, as users have to generate or distribute contents to be able to socialize. Again, it seems that 'social' information is disclosed rather less to get services for free, customised services or offers. This points once more at the distinction between the 'commercial' and the 'social' in SNS, in the eyes of their users; it also points at the relevance in this respect of concepts of 'purposefulness' of data provision and limited reuse of personal data that lies at the heart of the data protection directive. Having said this, more people provide commercially valuable information on SNS than people provide social information on eCommerce sites. This may point to an advantage of SNS operators over eCommerce providers regarding viability of business plans based on Web2.0 dynamics – extracting monetary value from people's personal information.

We then checked reasons to disclose by country and by socio-economic characteristics of SNS users.[38] In terms of countries, we found no significant regional pattern. In terms of socio-demographic characteristics, again we found limited variance: people from different background appear to disclose on SNS for similar reasons. The only small difference concerns young people who are slightly more likely to disclose information for fun and to connect with others.

35 In the Appendix, Table 52, Table 54 report country-level values of discrete indicators as to willingness to disclose.

36 The questions were asked as not to influence the responder, that is first asked what information is personal data from a list and then, in context, what has been disclosed from the same list.

37 QB5a: What are the most important reasons why you disclose such information on social networking sites and\ or sharing sites? is reported in Section 3.9.

38 Tables 52 – 55 in Section 3.9 provide country and socio-demographic breakdowns of different reasons to disclose in SNS.

Table 36. Data disclosure in SNS by what is personal data

People who disclosed…		% who consider it personal
Financial information	No	78
	Yes	84
Name	No	40
	Yes	46
Photos	No	50
	Yes	52
Nationality	No	24
	Yes	29
Activities	No	24
	Yes	28
Who friends are	No	30
	Yes	35
Address	No	64
	Yes	60
Preferences	No	27
	Yes	30
Work history	No	30
	Yes	33

Base: SNS users.

Source: QB4a and QB2.

Notes: Mobile phone, website visited and national identity number had no significant differences.

Only items disclosed by more than 6% of people are reported. Differences reported are significant at $p < 0.001$.

Table 37. Reasons to disclose information in SNS by items disclosed

	To access the service	To save time at the next visit	To receive money or price reductions	To benefit from personalised commercial offers	To get a service for free	To obtain a service adapted to your needs	For fun	To connect with others
Overall	61%	12%	6%	8%	17%	17%	23%	54%
Financial information	68%	24%	18%	17%	25%	26%	14%	34%
Work history		17%	9%	15%		23%		58%
National identity number	74%	23%	13%	16%	25%	26%	14%	33%
Name	64%		5%	7%				56%
Address	72%	19%	9%	11%	22%	24%	16%	45%
Nationality	65%	14%		9%	20%	20%	25%	59%
Activities	59%		5%	7%			32%	68%
Preferences							33%	67%
Photos	59%	10%	4%	6%	16%	16%	31%	67%
Friends	59%	10%	4%	5%		16%	33%	72%
Web visited	66%	17%		11%	22%	25%	30%	63%
Mobile	74%	18%	9%	12%	25%	24%	18%	49%

Base: SNS users.

Source: QB5b.

Note: Only items disclosed by more than 6% of people are reported. Only differences that are significant at p<0.001 are reported.

3.6 Risks of data disclosed in SNS[39]

Overall, virtually all respondents (98%) perceive some sort of risk connected to SNS disclosure [Table 38]. It is true however that different people perceive different risks, and that these do not cluster neatly, as other variables were reported to do (i.e. risks are seen are rather dissimilar and discrete by respondents). SNS users are likely to consider use of their information without their knowledge the greatest risk in SNS (44%), followed by fraud (41%). 'Your information being shared with third parties without knowledge' is the next most important risk (38%). They are also likely to consider identity being at risk of theft online (33%). Personal safety is perceived as a lesser issue (20%); as well as views and behaviours being misunderstood (11%) and being discriminated against (e.g. in job selection, receiving price increases, getting no access to a service) (7%).

It is interesting to compare these results with the risks perceived by people who use eCommerce [Figure 11; also see Table 15 on page 38]. The ranking of respondents' risk perceptions is very similar for social networking or sharing sites as for shopping online, with the exception of being the victim of fraud: this item is the second most important risk associated with social networking but the most important risk in the case of shopping online (41% versus 55%). Other risks are mentioned more for social networking than for shopping online: personal safety being at risk (20% and 12% respectively), reputation being damaged (12% and 4%), views and behaviours being misunderstood (11% and 4%), and discrimination in areas like recruitment, pricing, or availability of services (7% and 3%).

Table 38. Risks from disclosing information in SNS

	% of SNS users
Your information being used without your knowledge	44
Yourself being victim of fraud	41
Your information being shared with third parties without agreement	38
Your identity being at risk of theft online	33
Your information being used to send you unwanted commercial offers	27
Your personal safety being at risk	20
Your reputation being damaged	12
Your views and behaviours being misunderstood	11
Yourself being discriminated against (e.g. in job selection)	7
None (SPONTANEOUS)	2

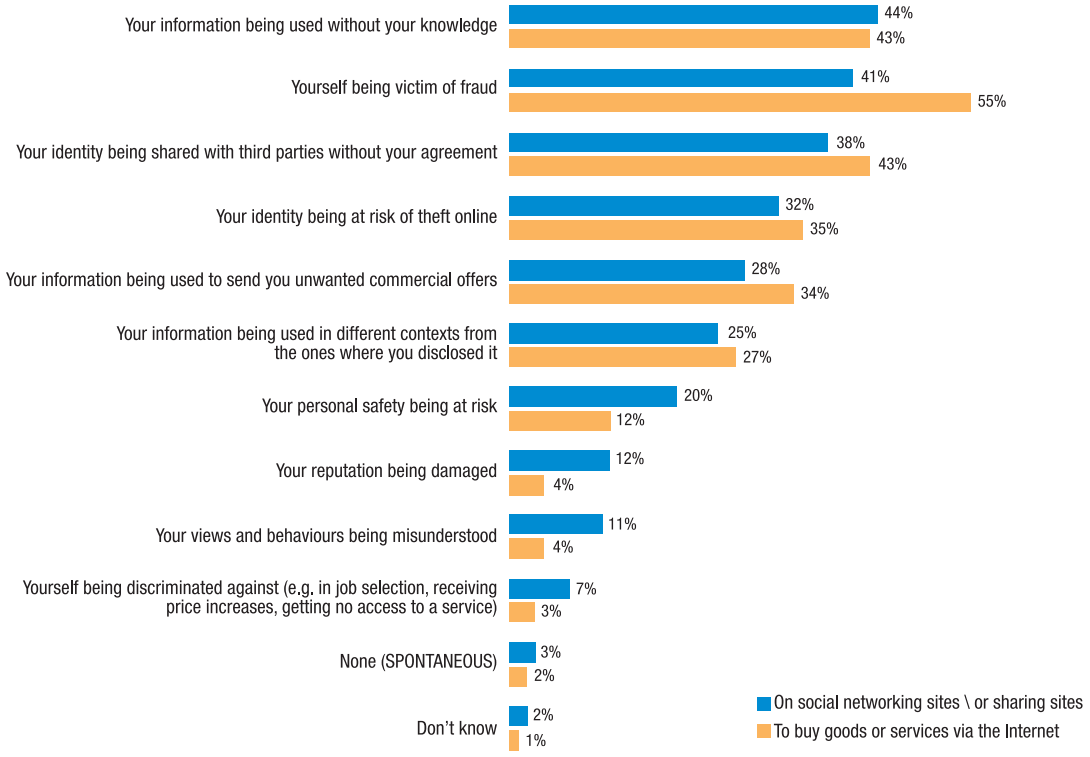
Source: QB7a.

Base: SNS users.

Note: Only differences that are significant at p<0.001 are reported.

39 QB7a. I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information on social networking sites and\ or sharing sites?

Figure 11: Perception of risks in SNS vs eCommerce



QB7: Basis: SNS users (40% of whole sample) and online shoppers (39% of whole sample).

It thus seems that the nature of the transaction environment [monetary vs. social], which is in turn related to the data actually disclosed, determines only in part the perception of different types of risk – apart from specific risks. And even for these specific risks [reputation on the one hand, fraud on the other], differences are not as large as it may have been expected.

It is then interesting to examine perceived risks in relation to the information people actually disclosed on SNS, in terms of number and in terms of type of information disclosed – traditional identifiers, social information and sensitive information [Table 39]. Results are surprising. Overall, there is no positive association between high perception of risk and low disclosure, across almost all the risks people mentioned and across types of information people disclosed; this mean that people disclose regardless of risk. So risks do not constitute a deterrent to disclosure. What is more, for commercial-procedural risks and for risks to reputation, there is a small, positive relation; this means that people who perceive these risks actually disclose more of their social and sensitive data. This may depend on increased alertness to risks once people have actually disclosed information about themselves. This is confirmed by a relatively robust correlation [r = .19] for overall number of risks perceived and number of personal data items disclosed in SNS. However, on the bright side, sensitive information show mixed correlations with a number of risks, namely it is negatively related to commercial – procedural risks, and to overall number of risks perceived; risks in this case may actually make people more cautious in releasing sensitive information.

To conclude, we should note that the questionnaire did not measure risks that may have prevented people to sign up for SNS in the first place; some people [not young people, obviously], may be put off by the risks mentioned and not take up SNS. But once they do take up SNS, then risks do not seem to be a deterrent to people disclosing their personal data, as described above. In the last section, we will

Table 39. Perceived risks in relation to SNS disclosure

	# SNS items disclosed	Traditional identifiers	Social information	Sensitive information
Your information being used without your knowledge		0.06		-0.06
Your information being shared with third parties without knowledge	0.06	0.05	0.06	
Your information being used to send you unwanted commercial offers	0.04	0.05		
Your information being used in different contexts	0.05	0.06	0.04	-0.05
Your identity being at risk of theft online				
Your personal safety being at risk				
Yourself being victim of fraud		0.04		
Yourself being discriminated against	0.05		0.06	
Your views and behaviours being misunderstood	0.06		0.08	0.06
Your reputation being damaged	0.05		0.06	0.07
Index of risk of disclosure in SNS [0-3]	0.19	0.13	0.15	-0.04

Source: QB4a and QB7a.

Base: SNS users who disclosed information.

Notes: Only significant relations at $p < 0.001$ are reported [i.e. when there is a 99.9% probability that the relation is not due to chance].

Results reported are:

1. Pearson's correlation coefficient for pairs of factors and/or scales.

2. Point-biserial correlation for factors and/or scales crossed by values.

3. Phi for relations between values, when they can be considered as multiple categorical (e.g. colour: white, red, or green).

examine the overall perception of SNS users regarding the Internet, to see if people who then go on to disclose on SNS are more likely to happily disclose in general, or if this behaviour is limited to their SNS frequentation.

In terms of socio-demographics, older SNS users are more likely to be concerned about the use of their information (information being shared with third parties without agreement; information being used to send unwanted commercial offers); younger SNS users are rather likely to worry about the impact of these uses [Figure 12]. Respondents aged 40-54 are more likely to mention the use of their information without their knowledge (48%) and their information being shared with third parties without their agreement (43%), whereas the oldest respondents (aged 55+) are more likely to mention their information being used to send them unwanted commercial offers (35%) and the risk of online identity theft (37%). This last item is also more often seen as a risk by respondents who left school at the age of 15 or younger (37%) than by those who remained longer in education.

More in general, education and occupation also make a difference. Manual workers and house persons (both 45%) are most likely to report that they fear becoming a victim of fraud; managers and house persons (both 42%) are most likely to mention their information being shared with third parties without their agreement, compared to 34% among students. Self-employed respondents (32%) more often cite the risk that their information may be used to send them unwanted commercial offers, and this item is also mentioned more frequently by retired respondents (36%), after the risk of identity theft (38%) and the use of their information without their knowledge (50%).

Figure 12. Risks from disclosure in SNS by socio-demographic profile

	Your information being used without your knowledge	Yourself being victim of fraud	Your information being shared with third parties without your agreement	Your identity being at risk of theft online	Your information being used to send you unwanted commercial offers	Your information being used in different contexts from the ones where you disclosed it
EU27	44%	41%	38%	32%	28%	25%
Sex						
Male	44%	42%	38%	31%	28%	25%
Female	44%	41%	38%	33%	27%	25%
Age						
15-24	43%	39%	35%	31%	24%	24%
25-39	42%	44%	38%	32%	28%	26%
40-54	48%	41%	43%	32%	29%	27%
55 +	46%	43%	37%	36%	35%	23%
Education (End of)						
15-	40%	44%	33%	37%	24%	18%
16-19	44%	43%	39%	32%	27%	25%
20+	45%	43%	41%	34%	31%	26%
Still studying	44%	35%	34%	31%	25%	26%
Respondent occupation scale						
Self-employed	45%	38%	38%	27%	32%	26%
Managers	44%	42%	42%	32%	30%	27%
Other white collars	45%	43%	41%	31%	29%	25%
Manual workers	43%	45%	36%	35%	26%	25%
House persons	43%	45%	42%	31%	26%	24%
Unemployed	39%	42%	38%	32%	22%	23%
Retired	50%	43%	37%	38%	36%	21%
Students	44%	35%	34%	31%	25%	26%

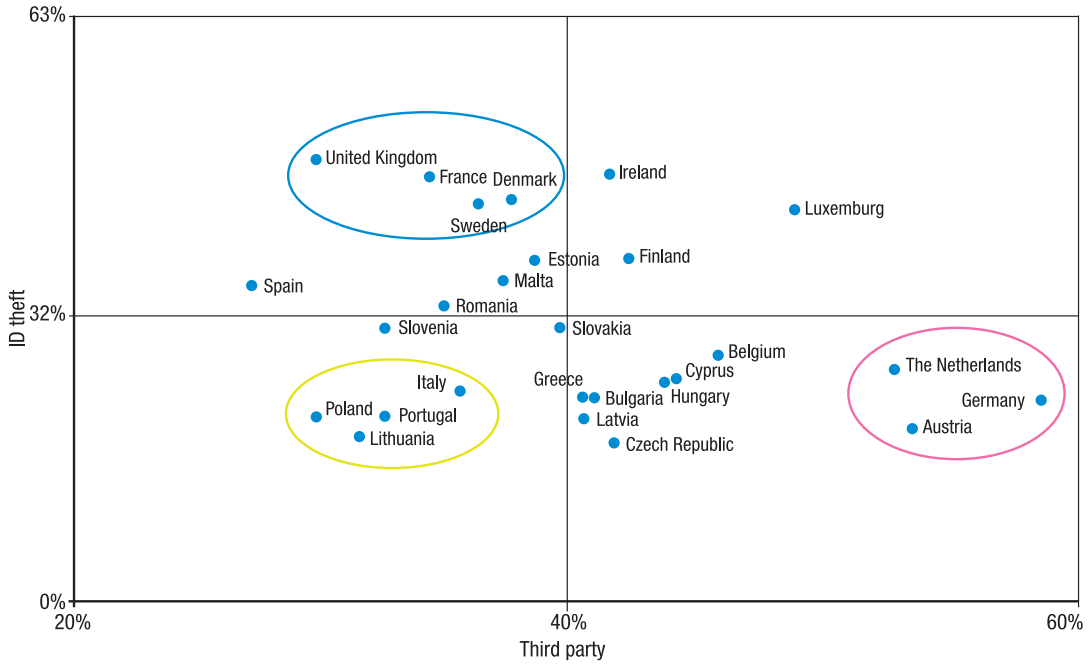
Source: QB7a.
Base: Social networking site users (40% of whole sample).

Concerning country difference, we looked at the issue in a more structured fashion, as difference for all these possible risks by EU27 are intricate.[40] In general, very different risks are perceived in different countries. We mapped differences for 'identity theft' and 'unauthorised third party use', as they both imply the intervention of a third party in the handling of one's data, and are both high in people's concern [Figure 13]. Among the high variance noted above, there appear to be three groups of countries that stand out. First, in some countries there are high perceived risks of unauthorised re-use of personal data, but low perceived risk of identity theft on SNS [The Netherlands, Germany, Austria]. People in these countries may assume that SNS are internally safe but controlled environments. In a second group, there are high perceived risks of identity theft, but low perceived risks of unauthorised reuse of personal information disclosed in SNS [UK, France, Sweden, Denmark]. In these countries, people may trust SNS operators more than the average EU citizen. Finally, there are countries where both the mentioned risks are below EU27 average [Poland, Lithuania, Portugal, Italy]. To further test these points, we constructed a scale of perceived risks, to see how countries fare against each other overall [table not reported].[41] SNS users living in the north of Europe, specifically Germany, Sweden, France, Ireland and Denmark

40 The interested reader may look at Table 56 in Section 3.9, for figures on perception of risks from disclosing personal information in SNS in each country.

41 As only three choices were given to respondents, out of ten possible risks, most people will have mentioned three risks [76% of SNS users]. However, we assume that SNS users who mentioned one or two risks, rather than three, have a lesser perception of threat. Of course, it may be the case that people only mentioned one risk as they though it overshadowed others. After checking, the similarity of response of the three types of respondents is remarkable. The only difference regards the slightly higher propensity for people reporting 'fraud' as one single risk.

Figure 13. Risk of identity theft and third party re-use of personal data in SNS by country



appear to have more concerns about SNS risk, as measured by the number of times mentioned [2.8 to 2.9 average]. Conversely, residents of Italy, Romania, Poland and Portugal [2.3 to 2.4 average], that is mainly the south-east of Europe, are likely to perceive lesser risk in SNS activity.

3.7 Control on data disclosed in SNS

A key concept in relation to personal data disclosure is that of control: how much control SNS users think they have on data they disclose. Control is a key component of the data protection framework, one that may be enabled and to some degree enforced by technical means and solutions on SNS and, overall, on the Internet. SNS users were asked about how much control they feel they have over the information disclosed on these sites.[42] A total of 26% of them stated that they feel they have complete control; 52% partial control and 20% no control at all.[43] Overall, individuals tend to feel more in control over 'social' information they disclose – such as

Table 40. Perception of control disclosing personal information by age

	15-24	25-39	40-54	55+
Complete control	31%	25%	24%	22%
Partial control	54%	54%	50%	48%
No control at all	14%	21%	26%	30%

Base: SNS users.

Source: QB6a.

Note: All differences are significant at $p < 0.01$.

42 Question QB6a. How much control do you feel you have over the information you have disclosed on social networking sites and\or sharing sites, e.g. the ability to change, delete or correct this information?

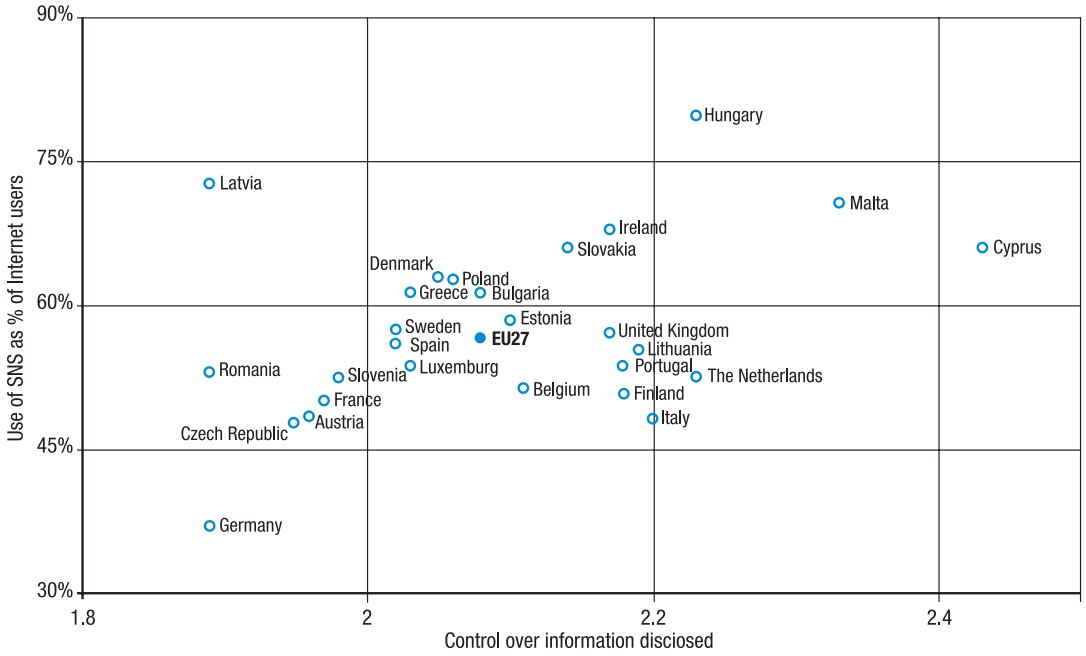
43 2% of SNS users answered 'Do not know'.

photos, preferences or activities – than when they disclose 'sensitive' information – such as financial or medical – or traditional 'identifiers' – such as mobile number or address [Table 59, in Section 3.9]. We then crossed perception of control by age [Table 40] and level of education [Table 60, in Section 3.9]. There are significant differences concerning age: very young and young users are more likely to feel they have complete or some control over the information they disclosed. Also, better educated SNS users are more likely to feel more control over the information. Nevertheless due to age, SNS users who are still studying are more likely to also feel more control.

Finally, we noted no consistent regional patterns; SNS users in Cyprus, Malta, and The Netherlands tend to report higher perceived control on their personal data; conversely, respondents in Germany, Latvia and Romania report lower control on the personal data they have disclosed in SNS. Difference may be due to the uptake of different SNS services in these countries [see Figure 6 and Figure 8]. We thus checked for network effects, to see if SNS uptake in a country was in any way related to feeling of control. The point is that people may feel more in control if more of their friends are online, or if a technology is seen as mature. It is interesting that this is indeed the case: a relation exists between uptake of SNS as % of internet users in a country, and feeling of control on information disclosed [r = .41, see Figure 14]. This holds true for age in general, and for all age groups except SNS users who are 55+ years old. This could be due to classical network effects [linked to increasing numbers]; it may be linked to technology maturity or to uptake of a particular SNS application across a group of countries. Survey data does not help us adjudicate between alternative explanations. However, feeling of control does increase as more and more diverse Internet users start using SNS [thus beyond the usual suspects: the digital natives].

Usually, perceptions of control are associated to what people actually disclose and to the risks perceived in relation to the information disclosure

Figure 14. Control on information disclosed in SNS and uptake at country level



Base: SNS users.
Source: QB6a.

Table 41. Control over information disclosed by actual disclosure, perceived risks and information

	Disclosure: social information	Disclosure: sensitive information	Disclosure: biography information	Index of risk of disclosure
Control on personal data disclosed	.06		-.10	-.07

Base: SNS users who disclosed information [control].

Source: QB6a.

Note: Only significant relations at $p < 0.001$ are reported [i.e. when there is a 99.9% probability that the relation reported is not due to chance]. Results reported are Pearson's correlation coefficient for pairs of factors and/or scales.

[Table 41].[44] Perceived control increases as people disclose more social information, but decreases in relation to the increased disclosure of biographical information; in other words, people may think they have more control on the social information they post to their profiles, than on the biographical information [name, address, mobile number] that is usually required to sign up for the service. The less is required, the more users feel in control over it. This may imply that minimisation of biographical information or use of encrypted, portable credentials for sign-up in SNS may increase user perceived control on their data. Finally, as it may be natural, the more risks people perceive associated with SNS activity, the less control they feel they have on the information they have disclosed. However, control is not associated to any specific risk.

3.7.1 Privacy settings in SNS

One practical tool in relation to control is the ability to change one's privacy setting on a SNS profile from default, to protect some or all of one's data from view. SNS users were asked about this.[45] Overall, 56% of SNS users stated that they have tried to change privacy settings of SNS personal profile from default options and 43% have not tried.[46] Thus, if SNS providers have not set appropriately high safeguards to protect people's personal data by default, a feat that not all operators accomplish,[47] just less that half of European SNS users may have left their personal data unprotected in these environments.

To investigate these further, SNS users who have not tried to change the default privacy settings, were probed about reasons why not [Table 42].[48] A total of 31% SNS users who have not tried reported that they trust the site to set appropriate privacy settings [which makes all the more important that these settings are appropriately, and not conservatively set]; 24% stated that they did not know that you could change the settings; 21% mentioned that they are not worried about personal data; and 20% do not know how to proceed with changing the settings. Finally, having the time to look at the available options was selected by 13% of the sample. Therefore, the most important reasons to not try to change privacy settings are firstly related with awareness and digital skills, and then trust in the SNS service provider.

Users who tried to change the default privacy settings were instead asked how easy or difficult

44 QB7a. I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information on SNS and\ or sharing sites?

45 QB10a. Have you ever tried to change the privacy settings of your personal profile from the default settings on a SNS?

46 1% Do not know.

47 "Assessment of the Implementation of the Safer Social Networking Principles for the EU on 14 Websites: Summary Report" June 2011 at: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report_11/part_one.pdf

48 QB12a. Why did you not try to change these privacy settings?

Table 42. Reasons why you did not try to change privacy settings

	% of SNS users who have not tried to change privacy settings
You trust the site to set appropriate privacy settings	31%
You did not know that you could change the settings	24%
You are not worried by having personal data on SNS	21%
You do not know how to proceed to change these settings	20%
You did not find the time to look at the available options	13%
Other (SPONTANEOUS)	7%
DK	5%

Base: SNS users who have not tried to change privacy settings.
Source: QB12a.

this was.[49] Most considered it very easy (36%) and fairly easy (46%); less than 15% stated that this change was fairly difficult or very difficult (3%). Thus, if the possibility is offered, users appear to be comfortable in contributing to protecting their personal data online.

3.7.2 Information about the possible consequences of disclosing in SNS

One of the key principles of the data protection framework in Europe is that of informed consent; regarding the 'informed' part, users have to be informed of the conditions of data collection and of the intended uses of the personal data they provide; SNS users were asked if SNS sites inform them about the possible consequences of disclosing personal information.[50] This question does not imply only information on the part of the user; it goes further in that it probes SNS operators' transparency concerning the risks and consequences that may affect users of the service [unforeseen by Directive 95/46]. SNS users appear to be split on this question: about half (49%) agree that they are sufficiently informed of possible consequences, but a similar proportion (46%) disagree.

We then looked at how the two concepts overlap: informed consent [gauged via QB17], and information about consequences in SNS. First, we note that among Internet users, SNS users are more likely to report that they have been informed of data collection conditions [Table 43].

This may not be extraordinary, as users of different online services report similar percentages (for instance, eCommerce, reported in the same table). However, more SNS users tend to report suitable information about collection conditions, rather than having been informed about possible consequences. We thus looked comparatively at the two types of information provided to SNS users [Table 44]. Largely, the two perceptions overlap [phi = .32, r = .24], but not to the extent that we expected. Table 44 can be divided in four quadrants. In red, 19% of all SNS users claim not have to been informed of either conditions or consequences. This is a clear area of action for the enforcement of Directive 95/46. In green, a significant proportion of SNS users [overall 29%] report having been informed; however, they are not happy with the degree of information about possible consequences. A relative majority in blue [40%] have been informed about collection conditions and consequences. And

49 QB11a. How easy or difficult did you find it to change the privacy settings of your personal profile?
50 QB8a. Please tell me whether you agree or disagree with the following statement: Social networking sites and\ or sharing sites sufficiently inform their users about the possible consequences of disclosing personal information.

Table 43. Informed about data collection conditions when disclosing personal data to access an online service

		Never	Rarely	Sometimes	Always
SNS	No	22%	18%	37%	23%
	Yes	12%	17%	41%	29.5%
eCommerce	No	20.5%	18%	38%	23.5%
	Yes	12.5%	17%	41%	40%
Total	Yes	15.5%	17.5%	40%	27%

Base: Internet users.

Source: QB1.2 & QB1.3 by QB8a.

Note: Figures are approximated to the closest half integer.

Table 44. Informed consent in online services by informed on consequences in SNS

		SC sites sufficiently inform their users about the possible consequences of disclosing personal information				
		Totally disagree	Tend to disagree	Tend to agree	Totally agree	Total
Informed about data collection conditions when disclosing personal data to access a service	Never	5%	4%	3%	2%	14%
	Rarely	4%	6%	4%	2%	16%
	Sometimes	5%	13%	19%	3%	40%
	Always	4%	7%	13%	7%	30%
	Total	18%	30%	39%	13%	100%

Base: SNS users.

Source: QB8a by Q17.

Note: Figures are approximated to the closest half integer.

a small group in brown [11%] are happy about SNS sites informing them of consequences, but have hardly been given information on how the data collected will be used [which may depend on the distinction between SNS sites and other online services].

Overall, the picture is not reassuring for the policymaker, as significant work is required to enforce informed consent and enhanced information about what may happen with people's personal data once it is disclosed. Also, results confirm what mentioned above: that more work is needed on the second count, and that sufficient information on possible consequence is a step further [therefore less frequent] than informed consent.

This line of reasoning leads us to check the relation of informed consent, information about possible consequences with the degree of control people have on data disclosed in SNS. Namely, we wish to determine which of the two types of information is more strongly related with feeling of control on the data disclosed [Table 45]. First, the feeling of control increases both in relation to increased information on uses of data and to information on possible consequences. Second, the feeling of control increases more rapidly in relation to increased feeling of information regarding possible consequences. Third, feeling of control grows the fastest for people who are fully informed about uses, and are informed about consequences. To compound the picture, we found that information about possible

Table 45. Control on personal data disclosed by informed consent and by information about consequences of disclosure

		Informed about consequences			
		Totally disagree	Tend to disagree	Tend to agree	Totally agree
Informed about data collection conditions	Never	1.7	1.9	2.1	2.3
	Rarely	1.8	1.9	2.0	2.3
	Sometimes	1.8	2.0	2.1	2.3
	Always	1.9	2.0	2.3	2.5

Base: SNS users.

Source: qb6a by QB8a x Q17.

Note: Figures reported are mean values of 'control'; 'control' is measured on a 1-3 scale, where 1 is no control at all over data one has disclosed in SNS, and 3 is total control.

Table 46. Sites sufficiently inform their users about the possible consequences of disclosing personal information by country

	Total 'Agree'
Portugal	76%
Italy	69%
Hungary	69%
Malta	67%
Ireland	63%
Rumania	60%
Poland	59%
Bulgaria	59%
United Kingdom	56%
Spain	56%
Lithuania	55%
Slovakia	54%
Estonia	54%
EU27	53%
Latvia	52%
Sweden	51%
Cyprus	50%
Finland	49%
Greece	48%
Austria	48%
Denmark	45%
Czech Republic	45%
Belgium	44%
Slovenia	43%
Germany	40%
The Netherlands	39%
France	36%
Luxemburg	33%

Note: p<0.001.

Base: SNS users.

Source: QB8a.

consequences has a negative relation with overall perception of risks in SNS [r = -.12]; the same is not true for information about the uses of data in online services [no significant correlation]. Overall, this means that while information overall is good at increasing people's feeling of control, contextual information about possible consequences has the strongest correlation with feeling of control on the information disclosed and decreases the overall perception of risks.

Concerning socio-economic status, we noted small differences only [table not reported]. Specifically, older people, people with university education, managers and very skilled internet users are more likely to disagree that SNS sites do a good job in informing them of possible consequences. On the other hand, there are significant country differences [Table 46]. While in EU27 about one in two people think they have been informed regarding consequences, at country level this ranges from two in three people in southern countries [Portugal, Italy, Malta, but also Hungary]; to one in three people in northern countries [Germany, The Netherlands, France, Luxemburg]. Once again country of residence [and of fruition of SNS service] is more important than individual socio-economic status traits to explain social SNS users' behaviours and perceptions.

3.7.3 Responsibility for personal data safety in SNS[51]

We then asked questions concerning who is perceived to be responsible for the safe collection, handling and storage of personal data online [Table 47].[52] It was surprising to see that most respondents claim they are personally responsible (49%), followed by site owners (34%) and by public authorities (17%). Results on who is responsible secondly largely confirmed this. Two thirds of people who say they are primarily responsible also think that online sites are responsible in the second place [conjoint table not reported]. Also, people who think shopping sites are primarily responsible also see an important secondary role for themselves. The structure of perceived of responsibility in SNS is clearly more tilted towards individuals and companies than the one people see in eCommerce [see also 2.6 on page 36].

Therefore, people feel responsible even if, as we pointed out above, they think they only have partial control on what they disclose and perceive

Table 47. Responsibility for personal data safety in SNS

	Firstly	Secondly
You - as you need to take care of your information	49%	27%
The social networking sites - as they need to ensure they process your information fairly	34%	42%
Public authorities - as they need to ensure that citizens are protected	17%	30%
DK	1%	2%

Base: SNS users.

Source: QB9a1, QB9a2.

51 QB9a1. Who do you think should make sure that your information is collected, stored and exchanged safely on social networking sites and\ or sharing sites? Firstly? and QB9a2. Secondly?

52 See question QB8b.

Table 48. Responsibility for personal data safety in SNS by perception of control

	Complete control	Partial control	No control at all
You	58%	48%	44%
SNS sites	32%	36%	33%
Public authorities	10%	16%	22%

Base: SNS users.

Source: QB9a1.

Table 49. Responsibility for personal data safety in SNS and information about possible consequences

	Informed about consequences	
	Total 'Disagree'	Total 'Agree'
You	44%	56%
SNS sites	49%	51%
Public authorities	55%	45%

Base: SNS users.

Source: QB9a1 and QB8a.

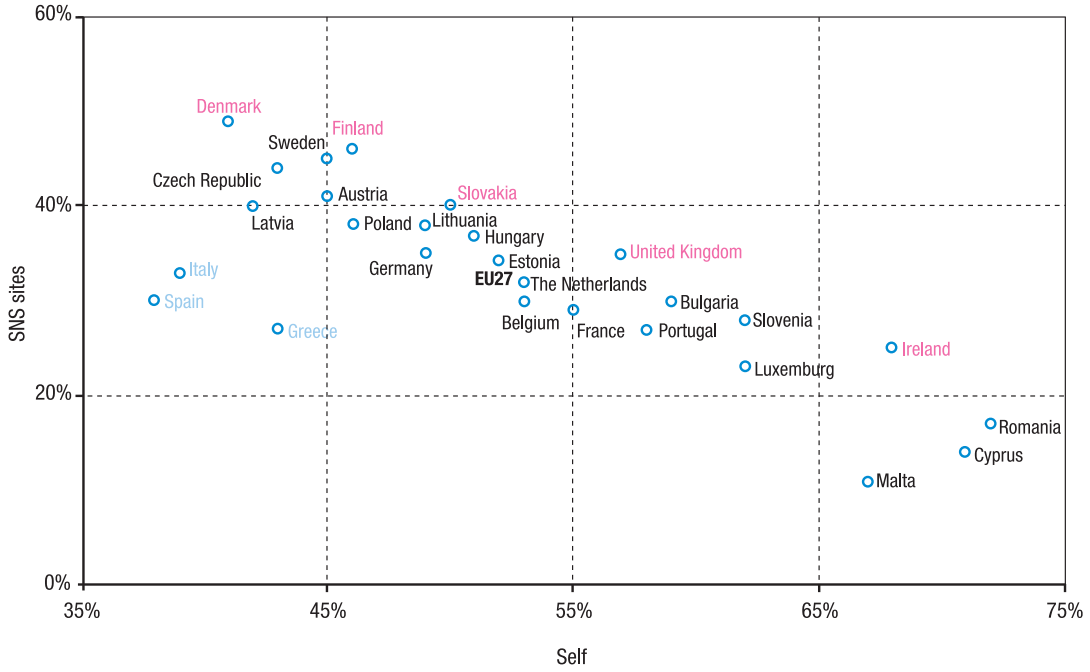
risks to be related to other parties' behaviours, rather than their own. But, we found significant differences in perceived responsibility and control [Table 48]. People who think they have no control on their personal data [again: once they've been disclosed], tend to see higher co-responsibility of industry and regulators. Conversely, those who think they have total control tend to see almost exclusive self-company responsibility. In all cases, companies are seen as responsible regardless of level of perceived control [e.g. their conferred responsibility remains relatively stable across perceived control].

It is no surprise that significant differences were also found in perceived responsibility and level of information provided about disclosing by SNS sites. SNS users holding that they are sufficiently informed are slightly more likely to perceive that they themselves or the SNS are responsible of personal data safety. Considering this, and considering the indirect influence of information of consequences on control we reported above, it may be wise for companies and policy-makers to foster full understanding of the working of personal data in SNS, if they wish to ensure that users take better care of their personal data.

Finally, we looked at socio-demographic and country difference in perceptions of responsibility [Section 3.9].[53] There are very few differences overall, which mainly relate to age. Concerning self responsibility, if anything, older SNS users tend to consider themselves responsible. Older people also hold public authorities more responsible than other SNS groups. On the other hand, younger people are more likely to consider SNS site responsible, while older people to consider them less responsible. Concerning country differences, there are four interesting tales [Figure 15]. First, [top left corner], there are countries where people consider SNS sites mainly responsible, and themselves much less so [Denmark, Latvia,

53 For clarity in the assessment of the relation between responsibility, SES and other variables, we employ a single composite measure of responsibility; we give a value of '2' to people who attribute first responsibility to any of the agents mentioned [self, site, authorities]; and a value of '1' to people who attribute secondary responsibility to these agents. Then, we check this measure for every agent against country of residence and socio-economic traits.

Figure 15. Responsibility to protect personal data disclosed by country



Sweden, Finland, Czech Republic]. Second, in some countries people feel personally responsible to protect their own data, and SNS sites much less so [Romania, Cyprus, Malta, Ireland]. Third, regardless of views on self vs. company, in some countries there is less support for public authority responsibility [Ireland, UK, Denmark, Finland, Slovakia]. We may call this lack of demand for public authority supplementation. Fourth, in some specific countries where people are not seen as responsible, public authority responsibility is the highest [Spain, Italy and Greece]. We may call this "substitution" of responsibility.

3.8 Relations with other variables

Table 50. Correlations between SNS-related variables and other relevant variables

Variables			Disclosure				Risks			Responsibility			Control
	Measurement		3 Factors				4 Values			3 x 3-point scales			3-point scale
		Values	Social information	Sensitive information	Traditional identifiers	Stealth use	Unwanted offers	Identity theft	Fraud	Self	Company	Authorities	
Attitudes towards disclosure	2 Factors	Unavoidability	-.11	-.04	-.11			-.04		.06		.-05	.07
		Propensity	-.09	-.10	-.09			-.07	.05		-.06	.04	-.13
Trust	2 Factors	Trust in institutions	.07		.07		.06			.06		-.05	.14
		Trust in companies		.04			-.05		-.05	.06	.05	-.05	.22
Concern about observation	1 Factor		-.09	.04					.06	-.07		.09	-.07
Use of credentials in daily life	2 Factors	Business-related	.19		.12	.04	.06	.07	.06	.05	.04	-.05	-.05
		Government issued			.12		.06	-.06				.08	-.10
Identity protection behaviours	4 Factors	Avoidance	.10	-.11	.06	.07	.06	.08	.06	.05		-.05	
		Adjustment	.13		.08	.08	.12				.04		-.04
		Low-tech	-.08					.04	.08		-.04	.04	
		Deception		.08			.04		-.04				
Internet identity protection	9-points scale		.17		.09	.04		.10			.06		
Awareness of identity theft and/or data loss	4 Values	Media awareness	.04		.05			.06	.05				-.34
		Social awareness	.05	.09						-.04			
		Self-family experience		.06				.04					
		No	-.05	-.07	-.05			-.06			-.04		.05
Comfort with online profiling	4-point scale		.06	.05		-.04			-.04			-.32	.15
Read privacy statements	3 Values	Read and understand								.05			.12
		Read no understand	-.07									.04	-.04
		No read	.1	-.04									-.09
Concern about reuse	4-point scale		-.11		-.04	.04		.07	.06	-.04	-.05	.08	-.08
Possibility to delete personal data	1 Value	Whenever one wants	.07	-.08	.05	.05				.05			
Importance of personal data portability	4-point scale					.04							.07

As the sample is large, only significant relations at $p < 0.001$ are reported [i.e. when there is a 99.9% probability that the relation reported is not due to chance].

Results reported are:

1. Pearson's correlation coefficient for pairs of factors and/or scales.

2. Point-biserial correlation for factors and/or scales crossed by values.

3. Phi for relations between values, when they can be considered as multiple categorical (e.g. colour: white, red, or green).

3.9 Additional tables and figures for SNS use

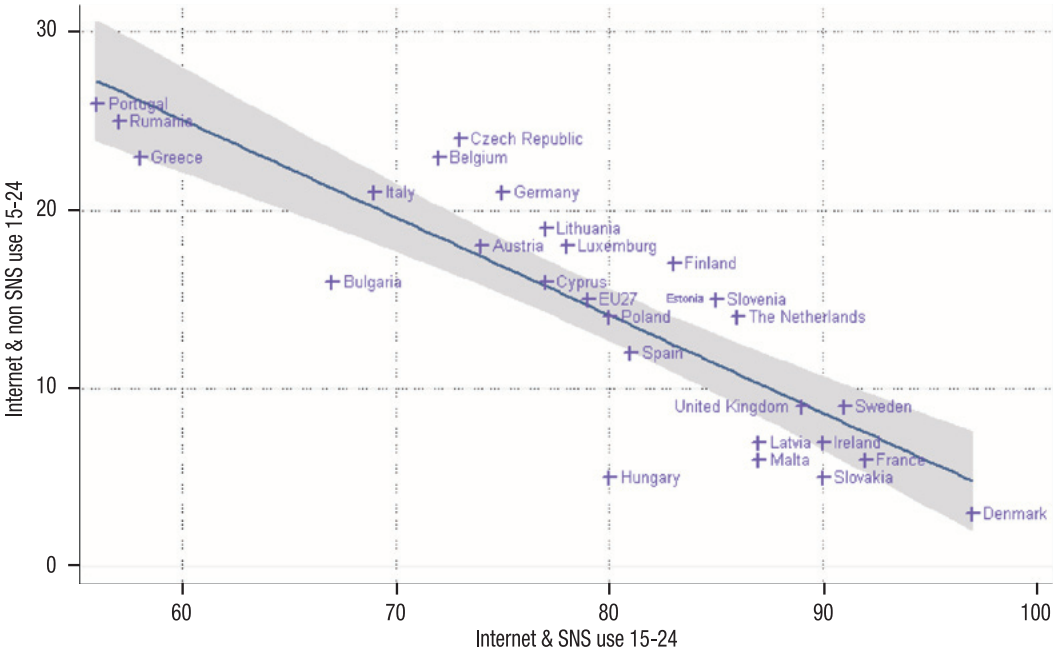
Table 51. SNS users and Internet activities

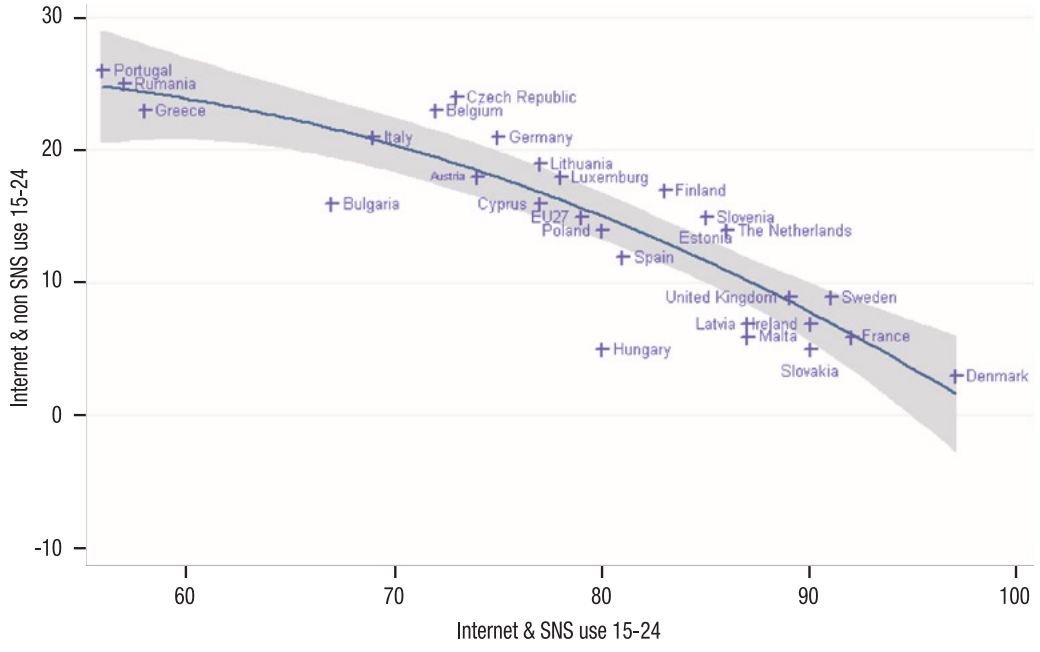
	% of SNS users also doing other activities
Use websites to share pictures, videos, movies, etc.	68%*
Instant messaging, chat websites	61%*
Purchase goods or services online	57%*
Home banking	50%*
Make or receive phone calls or video calls over the Internet	32%*
Use online software	30%*
Use peer-to-peer software and\ or sites to exchange movies, music,	22%*
Install plug-ins in your browser to extend its capability	17%*
Keep a blog (also known as web-log)	10%*
Design or maintain a website (not just a blog)	9%*

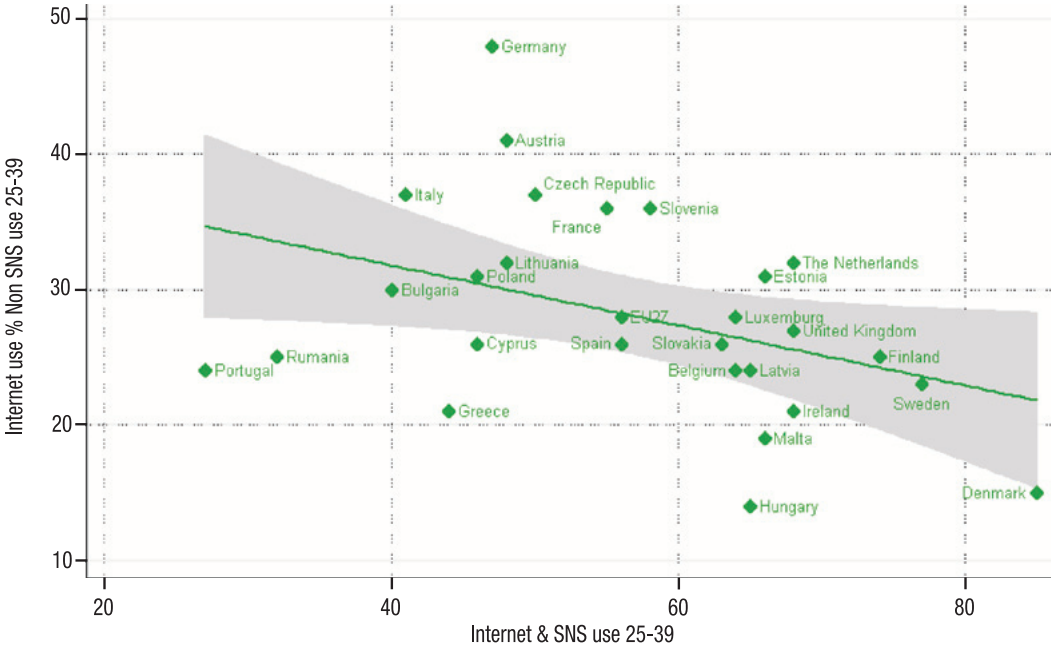
Source: QB1b. Which of the following activities do you also do on the Internet?.

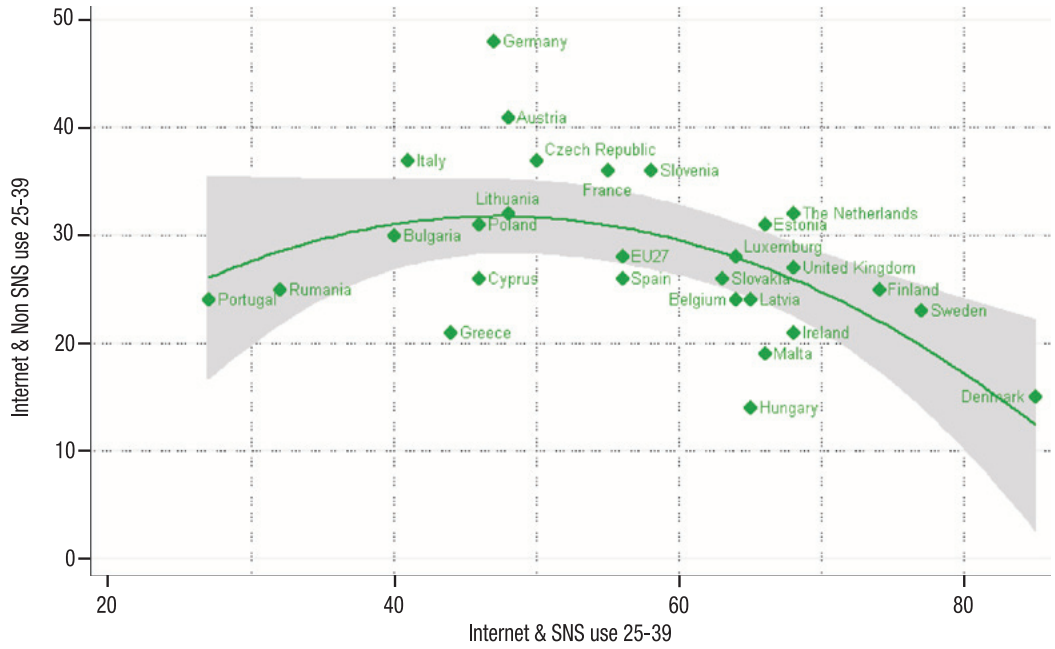
Base: Internet users.

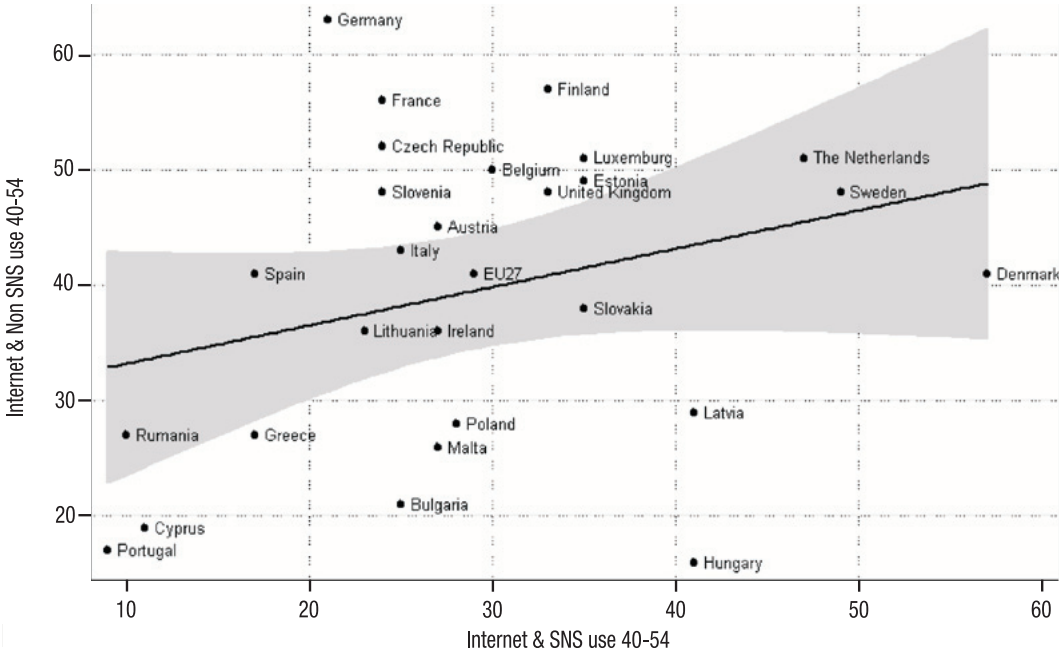
*Notes: * p<0.001.*

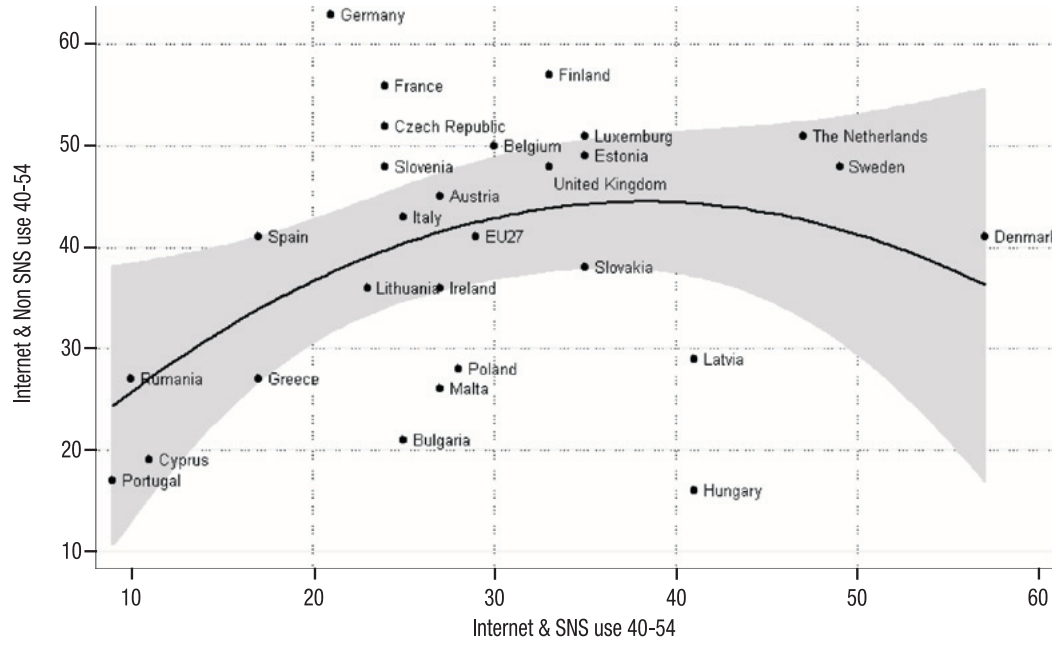

Internet & non SNS use 15-24
Internet & SNS use 15-24
30
20
10
0
60
70
80
90
100
Portugal
Rumania
Greece
Czech Republic
Belgium
Italy
Germany
Lithuania
Austria
Luxemburg
Finland
Bulgaria
Cyprus
EU27
Estonia
Slovenia
Poland
The Netherlands
Spain
United Kingdom
Sweden
Latvia
Ireland
Malta
France
Hungary
Slovakia
Denmark

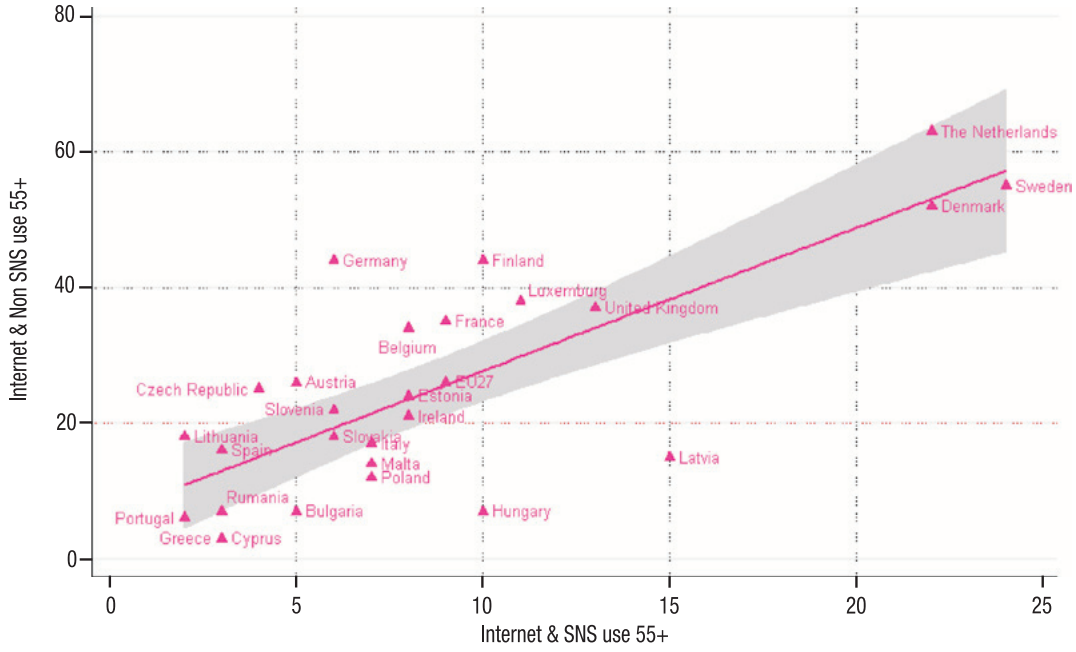

Internet & non SNS use 15-24
Internet & SNS use 15-24
30
20
10
0
-10
60
70
80
90
100
Portugal
Rumania
Greece
Czech Republic
Belgium
Italy
Germany
Lithuania
Austria
Luxemburg
Finland
Bulgaria
Cyprus
EU27
Slovenia
Poland
Estonia
The Netherlands
Spain
United Kingdom
Sweden
Latvia
Ireland
Malta
France
Hungary
Slovakia
Denmark


Internet use % Non SNS use 25-39
Internet & SNS use 25-39
50
40
30
20
10
20
40
60
80
Germany
Austria
Italy
Czech Republic
France
Slovenia
Lithuania
Poland
Bulgaria
The Netherlands
Estonia
EU27
Luxemburg
United Kingdom
Cyprus
Spain
Slovakia
Finland
Rumania
Portugal
Belgium
Latvia
Sweden
Greece
Ireland
Malta
Denmark
Hungary


Internet & Non SNS use 25-39
Internet & SNS use 25-39
50
40
30
20
10
0
20
40
60
80
Germany
Austria
Italy
Czech Republic
Slovenia
France
Lithuania
Poland
Bulgaria
The Netherlands
Estonia
Luxemburg
EU27
United Kingdom
Cyprus
Spain
Slovakia
Finland
Portugal
Rumania
Belgium
Latvia
Sweden
Greece
Ireland
Malta
Denmark
Hungary


Germany
France
Finland
Czech Republic
Luxemburg
Belgium
Estonia
The Netherlands
Slovenia
United Kingdom
Sweden
Austria
Italy
Spain
EU27
Denmark
Slovakia
Lithuania
Ireland
Latvia
Poland
Rumania
Greece
Malta
Bulgaria
Cyprus
Portugal
Hungary
Internet & Non SNS use 40-54
Internet & SNS use 40-54
10
20
30
40
50
60


Germany
France
Finland
Czech Republic
Luxemburg
Belgium
Estonia
The Netherlands
Slovenia
United Kingdom
Sweden
Austria
Italy
Spain
EU27
Denmarl
Slovakia
Lithuania
Ireland
Latvia
Poland
Rumania
Greece
Malta
Bulgaria
Cyprus
Portugal
Hungary
Internet & Non SNS use 40-54
Internet & SNS use 40-54
10
20
30
40
50
60


Internet & Non SNS use 55+
Internet & SNS use 55+
0
20
40
60
80
0
5
10
15
20
25
The Netherlands
Sweden
Denmark
Germany
Finland
Luxemburg
United Kingdom
France
Belgium
Czech Republic
Austria
EU27
Estonia
Slovenia
Ireland
Lithuania
Spain
Slovakia
Italy
Malta
Poland
Latvia
Rumania
Portugal
Bulgaria
Hungary
Greece
Cyprus

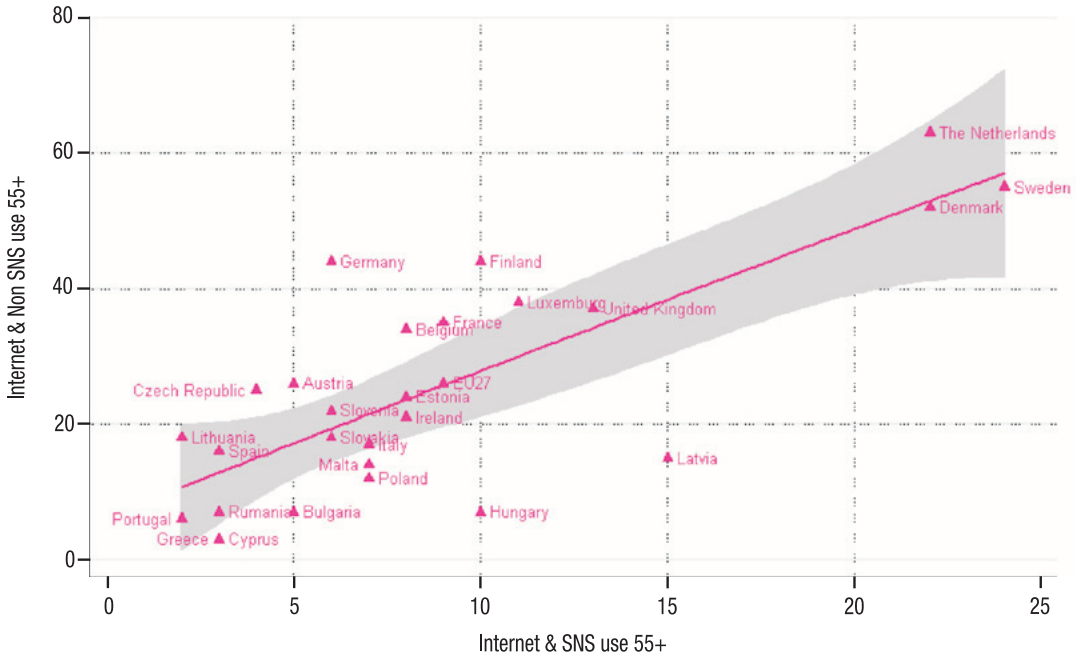

Internet & Non SNS use 55+
Internet & SNS use 55+
0
20
40
60
80
0
5
10
15
20
25
The Netherlands
Sweden
Denmark
Germany
Finland
Luxemburg
United Kingdom
France
Belgium
Czech Republic
Austria
EU27
Estonia
Slovenia
Ireland
Lithuania
Spain
Slovakia
Italy
Malta
Poland
Latvia
Portugal
Rumania
Bulgaria
Hungary
Greece
Cyprus

Table 52. Disclosure of personal data in SNS by country

	Financial	Work history	National identity number	Name	Address	Nationality	Activities	Preferences	Photos	Who friends are	Website visited	Mobile number
Austria	23%	29%	13%	85%	52%	66%	52%	48%	62%	52%	30%	42%
Belgium	8%	26%	11%	89%	45%	66%	46%	35%	59%	50%	19%	22%
Bulgaria	5%	9%	15%	80%	26%	52%	46%	33%	57%	38%	20%	19%
Cyprus	10%	14%	11%	92%	43%	55%	28%	28%	55%	45%	13%	21%
Czech Republic	10%	11%	15%	90%	54%	43%	49%	35%	44%	34%	22%	41%
Denmark	11%	35%	23%	95%	46%	68%	46%	30%	69%	60%	15%	41%
Estonia	17%	17%	35%	89%	43%	49%	45%	25%	61%	47%	20%	39%
Finland	8%	18%	15%	93%	39%	68%	41%	44%	60%	34%	14%	29%
France	6%	36%	4%	83%	41%	49%	41%	38%	61%	49%	12%	22%
Germany	12%	24%	6%	84%	54%	62%	49%	34%	51%	39%	17%	25%
Greece	11%	9%	15%	77%	41%	34%	28%	31%	49%	33%	20%	19%
Hungary	14%	23%	14%	81%	53%	31%	37%	27%	49%	35%	17%	25%
Ireland	11%	17%	9%	87%	50%	63%	56%	42%	56%	46%	24%	26%
Italy	11%	17%	17%	74%	26%	53%	46%	38%	51%	43%	14%	15%
Latvia	15%	19%	29%	91%	40%	37%	38%	25%	60%	26%	16%	48%
Lithuania	4%	12%	6%	86%	34%	45%	41%	24%	63%	39%	29%	19%
Luxemburg	6%	35%	6%	89%	28%	72%	59%	45%	66%	60%	23%	12%
Malta	10%	14%	14%	84%	45%	78%	50%	47%	63%	46%	22%	17%
Poland	4%	6%	13%	85%	52%	37%	25%	18%	36%	24%	13%	34%
Portugal	12%	13%	18%	69%	31%	42%	32%	41%	43%	25%	14%	19%
Romania	13%	21%	15%	70%	42%	52%	39%	33%	50%	34%	16%	20%
Slovakia	11%	16%	21%	85%	59%	39%	48%	30%	55%	49%	21%	41%
Slovenia	7%	8%	11%	93%	57%	38%	42%	32%	58%	44%	24%	29%
Spain	17%	13%	28%	84%	40%	61%	48%	51%	51%	32%	15%	22%
Sweden	13%	30%	44%	97%	56%	70%	52%	39%	68%	58%	18%	46%
The Netherlands	7%	23%	8%	89%	38%	56%	58%	35%	65%	48%	14%	20%
United Kingdom	5%	11%	4%	85%	26%	39%	39%	39%	73%	58%	13%	13%
EU27	10%	20%	16%	86%	44%	53%	44%	35%	58%	44%	18%	29%

Note: p<0.001.

Base: SNS users.

Source: QB4a. Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?.

Table 53. Reasons to disclose information in SNS

	% of SNS users who disclose information
To access the service	61
To connect with others	54
For fun	23
To get a service for free	17
To obtain a service adapted to your needs	17
To save time at the next visit	12
To benefit from personalised commercial offers	8
To receive money or price reductions	6
Other (SPONTANEOUS)	1

Base: SNS users.

Source: QB5b.

Table 54. Reasons to disclose in SNS by country

	To access the service	To get a service for free	To obtain a service adapted to your needs	For fun	To connect with others
EU27	62%	17%	20%	22%	51%
Belgium	61%	13%	16%	27%	47%
Denmark	**74%**	21%	**29%**	18%	54%
Greece	55%	17%	22%	6%	57%
Spain	73%	23%	18%	17%	43%
Finland	68%	14%	24%	25%	59%
France	60%	11%	17%	23%	55%
Ireland	75%	13%	21%	28%	42%
Italy	61%	18%	17%	29%	44%
Luxemburg	45%	8%	17%	33%	**73%**
The Netherlands	50%	11%	14%	28%	**65%**
Austria	58%	**40%**	25%	20%	41%
Portugal	50%	13%	14%	27%	43%
Sweden	79%	10%	21%	39%	61%
United Kingdom	53%	7%	7%	28%	61%
Germany	60%	**33%**	25%	15%	62%
Bulgaria	56%	16%	16%	**36%**	55%
Cyprus	**79%**	14%	20%	14%	47%
Czech Republic	60%	14%	24%	27%	49%
Estonia	**70%**	18%	18%	7%	50%
Hungary	63%	15%	17%	16%	49%
Latvia	61%	14%	24%	24%	53%
Lithuania	58%	18%	18%	11%	59%
Malta	67%	11%	**33%**	22%	40%
Poland	69%	22%	19%	6%	34%
Romania	58%	22%	17%	18%	33%
Slovakia	56%	19%	25%	**32%**	51%
Slovenia	64%	18%	24%	11%	53%

Notes: p<0.001.

Only reasons mentioned by at least 15% of respondents were reported in the table.

Base: SNS users.

Source: QB5b.

Table 55. Reasons to disclose in SNS by socio-economic status

		To save time at the next visit	To benefit from personalised commercial offers	To get a service for free	To obtain a service adapted to your needs	For fun	To connect with others
	EU27	12%	8%	17%	17%	23%	54%
Age [brackets]	15-24	11%	6%	20%	15%	26%	58%
	25-39	13%	9%				56%
	40-54		10%	15%	21%	18%	48%
	55+	16%	5%			19%	47%
Terminal education age	15-		3%		13%	30%	48%
	16-19		9%				
	20+				21%	21%	52%
	Still Studying		6%		14%	26%	60%
Occupation	Self-employed	9%	13%		23%		44%
	Managers				20%	20%	
	Other white collars	14%	10%			21%	
	Manual workers				19%		
	House person	9%			13%		59%
	Unemployed	17%			13%		
	Retired						48%
	Students	11%	6%		14%	26%	60%
Personal mobile phone	No			8%			
	Yes			18%			
Difficulties to pay bills	Most of the time		11%				
	From time to time		9%				
	Almost never/ never		7%				
Household composition	1					28%	
	2						
	3			20%		21%	
	+4						

Notes: Only significant difference at p < 0.001 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Base: SNS users.

Source:Qb5b.

Table 56. Perception of risks of disclosing personal information in SNS by country

	Your information being used without your knowledge	Your information being shared with third parties without knowledge	Your information being used to send you unwanted commercial offers	Your views and behaviours being misunderstood	Your identity being at risk of theft online	Your personal safety being at risk	Yourself being victim of fraud	Yourself being discriminated against	Your reputation being damaged	Your information being used in different contexts
Belgium	47%	46%	34%	14%	28%	21%	28%	10%	9%	24%
Denmark	51%	38%	34%	12%	45%	15%	37%	6%	4%	44%
Greece	52%	41%	24%	14%	23%	15%	42%	4%	6%	25%
Spain	40%	26%	20%	11%	34%	31%	52%	5%	15%	17%
Finland	42%	41%	18%	7%	38%	27%	39%	4%	9%	45%
France	46%	33%	29%	9%	46%	18%	47%	12%	15%	18%
Ireland	61%	41%	22%	16%	46%	24%	35%	7%	8%	14%
Italy	41%	36%	25%	14%	23%	16%	26%	4%	10%	34%
Luxemburg	54%	46%	31%	14%	38%	15%	31%	8%	8%	15%
Netherlands	47%	53%	42%	15%	25%	12%	26%	5%	11%	29%
Austria	46%	54%	34%	16%	20%	14%	30%	11%	13%	32%
Portugal	31%	34%	24%	8%	19%	22%	56%	4%	9%	18%
Sweden	51%	37%	27%	12%	44%	15%	42%	11%	7%	39%
UK	35%	28%	17%	10%	48%	27%	49%	7%	8%	23%
Germany	42%	59%	34%	9%	22%	16%	41%	7%	16%	35%
Bulgaria	58%	38%	25%	14%	21%	21%	39%	1%	7%	18%
Cyprus	73%	43%	20%	13%	27%	33%	40%	7%	7%	20%
Czech Republic	52%	41%	42%	12%	18%	17%	40%	6%	14%	22%
Estonia	41%	38%	28%	7%	34%	31%	45%	7%	21%	10%
Hungary	57%	44%	37%	8%	24%	16%	32%	7%	11%	14%
Latvia	53%	41%	31%	7%	20%	19%	48%	6%	9%	19%
Lithuania	50%	31%	26%	7%	18%	23%	45%	4%	20%	18%
Malta	60%	33%	22%	11%	33%	20%	33%	10%	11%	22%
Poland	45%	29%	32%	7%	22%	14%	53%	3%	10%	23%
Romania	62%	32%	23%	13%	29%	14%	25%	2%	6%	10%
Slovakia	46%	41%	31%	17%	29%	26%	29%	6%	23%	18%
Slovenia	58%	34%	25%	10%	29%	19%	45%	6%	13%	31%
EU27	50%	39%	28%	11%	30%	20%	39%	6%	11%	24%

Note: p<0.001.

Base: SNS users.

Source: QB7a. According to you, what are the most important risks connected with disclosure of personal information on social networking sites and\ or sharing sites?.

Table 57. Perception of the necessity of disclosing personal information by country

	Nowadays you need to log into several systems using several usernames and passwords	The (NATIONALITY) Government asks you for more and more personal information	You feel obliged to disclose personal information on the Internet	There is no alternative than to disclose personal information if one wants to obtain products or services	Disclosing personal information is not a big issue for you	Disclosing personal information is an increasing part of modern life
Belgium	82%	60%	32%	61%	36%	73%
Denmark	94%	67%	54%	70%	56%	95%
Greece	83%	91%	51%	79%	30%	97%
Spain	85%	76%	58%	74%	41%	87%
Finland	97%	52%	53%	83%	38%	89%
France	80%	62%	33%	61%	25%	83%
Ireland	87%	74%	55%	76%	41%	87%
Italy	81%	86%	62%	71%	46%	89%
Luxemburg	73%	40%	36%	64%	27%	73%
The Netherlands	92%	68%	33%	70%	42%	76%
Austria	90%	68%	37%	81%	53%	85%
Portugal	73%	81%	44%	64%	47%	81%
Sweden	95%	44%	46%	70%	48%	91%
United Kingdom	88%	72%	52%	76%	31%	88%
Germany	94%	84%	32%	81%	39%	79%
Bulgaria	81%	76%	48%	79%	41%	85%
Cyprus	85%	67%	31%	75%	23%	85%
Czech Republic	87%	65%	64%	78%	38%	79%
Estonia	92%	48%	36%	75%	48%	88%
Hungary	79%	63%	30%	69%	35%	62%
Latvia	88%	49%	14%	76%	24%	83%
Lithuania	90%	52%	37%	57%	53%	77%
Malta	89%	38%	22%	67%	25%	67%
Poland	76%	70%	31%	75%	49%	88%
Romania	80%	64%	45%	56%	49%	67%
Slovakia	91%	60%	23%	73%	37%	77%
Slovenia	93%	77%	13%	63%	28%	85%
EU27	86%	65%	40%	71%	39%	82%

Note: p<0.001.

Base: SNS users.

Source: QB3. For each of the following statements, could you please tell me whether you totally agree, tend to agree, tend to disagree or totally disagree?.

Table 58. Perception of control disclosing personal information by education

How old were you when you stopped full-time education?	Complete control	Partial control	No control at all
15-	6%*	4%*	9%*
16-19	44%*	39%*	44%*
20+	25%*	33%*	34%*
Still Studying	25%*	23%*	13%*

*Note: *p<0.001.*

Base: SNS users.

Source: QB6a by terminal education age.

Table 59. Information disclosed by SNS users and control perception

	Complete control	Partial control	No control at all
Activities	27%	56%	17%
Preferences	27%	57%	16%
Photos	29%	55%	16%
Who friends are	28%	56%	16%
Websites visited	25%	59%	16%

Note: Only categories that display significant difference at p<0.001 are reported.

Source: QB4 and QB6a.

Base: SNS users.

Table 60. Perception of control disclosing personal information in SNS by country

	No control at all [1]	Partial control [2]	Complete Control [3]	Mean
Cyprus	7%	36%	57%	2.5
The Netherlands	10%	58%	32%	2.3
Malta	11%	44%	44%	2.3
Finland	10%	61%	29%	2.2
Ireland	15%	53%	32%	2.2
Italy	15%	50%	35%	2.2
Portugal	8%	66%	26%	2.2
United Kingdom	16%	50%	33%	2.2
Hungary	10%	57%	33%	2.2
Lithuania	13%	55%	32%	2.2
Belgium	21%	48%	31%	2.1
Denmark	21%	53%	26%	2.1
Bulgaria	18%	55%	26%	2.1
Estonia	15%	59%	26%	2.1
Poland	16%	61%	23%	2.1
Slovakia	14%	58%	28%	2.1
EU27	**18%**	**54%**	**28%**	**2.1**
Greece	23%	52%	26%	2
Spain	22%	55%	24%	2
France	29%	45%	26%	2
Luxemburg	17%	58%	25%	2
Austria	20%	63%	17%	2
Sweden	22%	53%	24%	2
Czech Republic	25%	56%	20%	2
Slovenia	25%	50%	25%	2
Germany	29%	52%	18%	1.9
Latvia	28%	56%	16%	1.9
Romania	29%	52%	19%	1.9

Table 61. Responsibility for personal data safety in SNS by socio-demographic traits

		You	SNS sites	Public authorities
	All SNS users	1.3	1.1	.6
Terminal education age	No full-time education	**1.5**	**.7**	**.8**
	15-	1.2	1.0	**.8**
	16-19	1.3	1.1	.6
	20+	1.3	1.1	.7
	Still Studying	1.2	**1.2**	.6
Gender	Male	1.2	1.1	.7
	Female	1.3	1.1	.6
Age	15-24	1.3	**1.2**	.6
	25-39	1.2	1.1	.6
	40-54	1.2	1.1	.7
	55+	1.3	**.9**	**.8**
Occupation	Self-employed	1.1	1.1	.7
	Managers	1.3	1.1	.6
	Other white collars	1.2	1.1	.7
	Manual workers	1.3	1.1	.6
	House person	1.3	1.1	.6
	Unemployed	1.3	1.1	.6
	Retired	**1.4**	**.9**	.7
	Students	1.2	**1.2**	.6
Personal mobile phone	No	1.2	**.9**	**.9**
	Yes	1.3	1.1	.6
Difficulty paying bills	Most of the time	1.2	1.1	.7
	From time to time	1.2	1.1	.7
	Almost never/ never	1.3	1.1	.6
Internet use access index	Low	1.3	1.0	.7
	Medium	1.3	1.1	.6
	High	1.2	**1.2**	.6

Base: SNS users.

Source: QB9a1, QB9a2.

Note: p<0.001.

Table 62. Responsibility for personal data safety in SNS by country

	You	SNS sites	Public authorities
Belgium	53%	30%	16%
Denmark	41%	49%	9%
Greece	43%	27%	30%
Spain	38%	30%	33%
Finland	46%	46%	8%
France	55%	29%	16%
Ireland	68%	25%	7%
Italy	39%	33%	29%
Luxemburg	62%	23%	15%
The Netherlands	53%	32%	15%
Austria	45%	41%	14%
Portugal	58%	27%	15%
Sweden	45%	45%	10%
United Kingdom	57%	35%	8%
Germany	49%	35%	16%
Bulgaria	59%	30%	11%
Cyprus	71%	14%	14%
Czech Republic	43%	44%	13%
Estonia	52%	34%	14%
Hungary	51%	37%	12%
Latvia	42%	40%	19%
Lithuania	49%	38%	14%
Malta	67%	11%	22%
Poland	46%	38%	16%
Romania	72%	17%	11%
Slovakia	50%	40%	10%
Slovenia	62%	28%	11%
EU27	52%	33%	15%

Base: SNS users.

Source: QB9a1, QB9a2.

Note: p<0.001.

4 FACT SHEET: Identity and Authentication in Europe

4.1 Question context

The questionnaire included various questions regarding identity management, both offline, and, to a large extent, on the Internet. In the order they are addressed in text, questions considered are:

Table 63. eID survey questions relevant to identity and authentication

Question code	Shorthand	Formulation	Rationale
QB14	Use of credentials	Which of the following do you currently use? Credit cards and bank cards Etc.	To determine the use of credentials in everyday life.
QB15	Identity protection behaviour	In your daily life, what do you do to protect your identity? Please indicate all that apply in the following list. Use cash instead of recorded transactions Etc.	To explore what people do, if anything, to protect their identity.
QB16	Online identity protection behaviour	And, specifically on the Internet, what do you do to protect your identity? Please indicate all that apply in the following list. Use a dummy email account Etc.	To explore what people do, if anything, to protect their identity online.
QB30	Awareness of data loss	In the last 12 months, have you heard about or experienced issues in relation to data losses and identity theft?	Awareness [personal, social media] of episodes of identity theft and data loss.

4.2 Legal context

Taking into account that identity management and authentication are not currently regulated by a specific and comprehensive piece of legislation at the EU level, the main legal instruments and policy initiatives with regard to electronic identity management are the following:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Specifically, the survey asks questions relevant to data loss and data breach notification,[54] which may assist the number of people that are happy to disclose personal data, that are less likely to minimise data and that rarely use software measures to protect their data. On the right balance to be stroke between enhanced control and self-protection and enforcement of actor-based rules. And on the relation between online identity management and people's regulatory preferences regarding data protection. Questions regarding the effective use of data subject's right of access to data in order to update it or delete it are also relevant for the current discussion on the so-called right to be forgotten and for a possible revision on how should such right be obtained from the controller.

- Directive 1999/93/EC on a Community framework for electronic signatures, and the proposal for a revision of the eSignature Directive with a view to provide a legal

54 "… the possible modalities for the introduction in the general legal framework of a general personal data breach notification, including the addressees of such notifications and the threshold beyond which the obligation to notify should apply" (in "A comprehensive strategy on data protection in the European Union", EC 2010).

framework for cross-border recognition and interoperability of secure eAuthentication systems [DAE Key Action 16]. The survey does not look specifically at the use of eSignature, as individual users' uptake is low across Member States; however, it looks at use of credentials and at strategies for protecting one's identity and transactions online, including in eCommerce [in MS, cross-border], eGov and SNS. This may assist the framing of the eSignature debate in wider terms.

- Directive 2006/123/EC on services in the internal market. The survey looks at the relation between identification mechanisms, online self protection and the fruition of eServices such as eCommerce, SNS and home banking.

- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

- Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

- The Consumer Rights Directive, still at proposal stage, which should replace and merge 4 existing consumers rights directives (Sale of consumer goods and guarantees (99/44/EC); Unfair contract terms (93/13/EC); Distance selling (97/7/EC); Doorstep selling (85/577/EC) and the revision of the EU data protection regulatory framework with a view to enhancing individuals' confidence and strengthening their rights [DAE Key action 4]. The survey examines issues of internet skills in relation to identity protection online and offline, and awareness of identity theft and data breach.

- The proposal for a Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector).

- EU Cookies Directive (Directive 2009/136/EC), namely the need for users to 'opt in' – that is consent following clear and comprehensive information. The survey queried strategies people use to protect their identity online (i.e. data on how many people delete cookies – 35%).

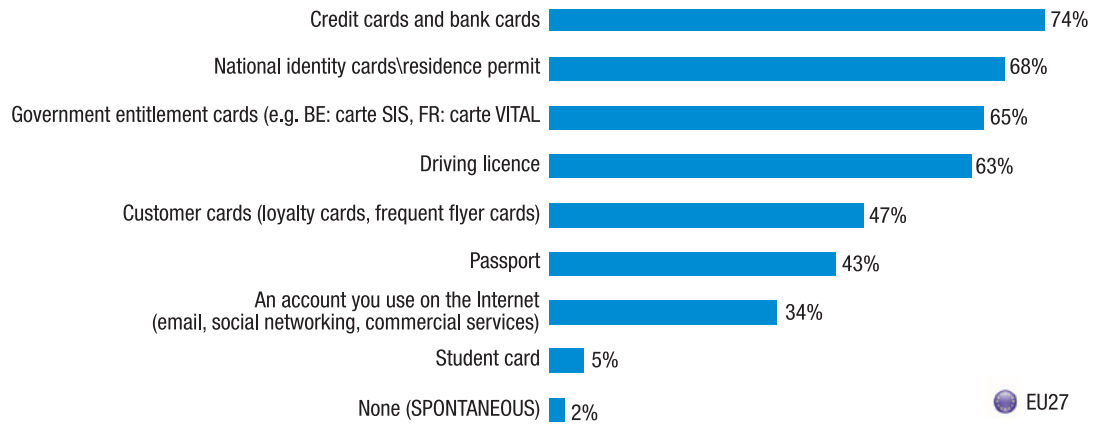
Before discussing how Europeans protect their identity in daily life and on the Internet, we examine the types of credentials they use, i.e. the types of identity papers and identity cards they usually use.

4.3 Use of credentials in Europe

Respondents were asked what personal credentials they use [Figure 16].[55] Almost three people in four use credit cards and bank cards (74%). Around two-thirds use national identity cards or residence permits (68%), government entitlement cards (65%) and driving licences (63%). About half of the interviewees use customer cards, such as loyalty cards and frequent flyer cards (47%), or a passport (43%). In terms of online credentials, about one in three European (one every two Internet users) also claim to use an Internet account (34%). This is consistent with other data in the survey that shows that about half

55 QB14: Which of the following do you currently use?

Figure 16. Use of credentials



Base: EU27.
Source: QB14.

Figure 17. Use of credentials crossed by use of SNS and eCommerce

	Credit cards and bank cards	National identity cards/ residence permit	Government entitlement cards (e.g. BE : carte SIS, FR : carte VITAL)	Driving licence	Customer cards (loyalty cards, frequent flyer cards)	Passport	An account you use on the Internet (email, social networking, commercial services)	Student card
Use a social networking site								
Yes	81%	62%	62%	67%	53%	50%	60%	13%
No	87%	66%	69%	79%	53%	54%	43%	2%
Purchase goods or services online								
Yes	91%	60%	69%	78%	59%	59%	62%	8%
No	74%	71%	61%	65%	45%	42%	38%	7%

Base: Internet users who also use Social Networking sites and eCommerce, respectively.
Source: QB14 by QB1b.

of EU internet users (52%) have an account on social networking or sharing sites.

It is interesting that respondents with high Internet-use are more likely to also use leisure-related credentials: driving license, customer cards, passports and Internet accounts, but less likely to use national identity cards. This points to the increasing embedding of credentials, more private than public, in the fabric of the Internet. This may only be natural, as government-issues credentials can be used to carry out online commercial transactions in a limited number of countries only, including Belgium, Austria, Spain and Estonia.[56] This is also confirmed by data on disclosure in eCommerce [2.7.1]: those who use government-related credentials are less likely to disclose personal information as they shop online [see eCommerce fact sheet, Table 25 on page 41].

56 Evidence in various figures in the report on "The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies" at: http://ftp.jrc.es/EURdoc/JRC60959.pdf as well as in the report on "Socio-Economic Assessment of selected EU eIdentity cross-border systems" (forthcoming).

Table 64. Factor analysis of credentials used in everyday life

	Factor 1. Business-related credentials	Factor 2. Government-related credential
Credit cards and bank cards	.74	
Driving licence	.71	
Passport	.65	
Customer cards	.60	
National identity cards/ residence permit		.86
Government entitlement cards		.62
Eigenvalue	2.03	1.23
% Variance explained	40	20.5

Source: QB14.

Base: EU27.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0.68; Bartlett's test of sphericity p=0.000; Convergence in 3 iterations; Minimum eigenvalue 1; Values below .4 are omitted.

Online shoppers and social networking and sharing site users are logically far more likely to use an account on the Internet than others [Figure 17]; for instance, 62% of online shoppers claim the use such an account, compared with only 38% of those who do not shop online. However, people who shop online are also far more likely to have credit and bank cards (91%), a passport (59%) and customer cards (59%). This will be further explored when looking at the socio-economic characteristics of people who actually use credentials online. On the other hand, it is striking that a significant proportion of respondents – including SNS and eCommerce users – claim they are not using an Internet account, while they carry out activities that clearly require one. Digital Natives are less likely to have credentials other than an Internet account and are thus much more aware of using their data. Much work needs to be done raising awareness of Interne users of the personal data they routinely provide to online service providers via their accounts, without being aware.

Further analysis explored the differences noted [Table 64]. Factor analysis examines whether people who use some credentials also use other credentials, in order to determine clusters of credentials used, or 'factors'. First, as we expected, we found two main types of credentials: business-related and government-related credentials. But then, we also found that passport and driving license, which are issued by governments, are used by people alongside other business-issued credentials. This may mean that in people's practice, the intended use – or function – of a credential [for instance: travel for the passport] is more salient that its issuer.

This is also interesting in relation with perceptions of risks in eCommerce [QB7b].[57] People who use business-related credentials are more likely to report a slightly higher perception of risk of identity theft and fraud due to eCommerce disclosure [r = .06]; conversely, people using government related credentials are likely to report reduced perception of risk of identity theft in eCommerce [r = -.12]. This may be natural: people are likely to associate higher risks to the loss of financial rather than governed-related information as it constitutes to them a greater and more visible asset. However, it is risky: with extended use

57 Risk factors associated with disclosure, p.57 of EB-359 report on Attitudes on Data Protection and electronic Identity, available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Table 65. Use of credentials in relation to Home Banking and eGovernment

	Home banking	eGovernment
Use of credit cards and bank cards	.28	.17
Use of customer cards	.21	.18
Use of national identity cards/ residence permit	-.05	-.05
Use of passport	.16	.13
Use of government entitlement cards	.11	.09
Use of driving licence	.21	.17

Source: QB14 by QB1b.

Base: Internet users.

Notes: results reported are Phi correlations. Only significant relations at $p < 0.001$ are reported [i.e. when there is a 99.9% probability that the relation reported is not due to chance].

of "phishing" techniques and by collating apparently un-related data, loss of government related data can prove as damaging as loss of financial data.

To further expand on the intertwining of credentials and Internet activities, we examined the relation of credentials with eGovernment online activity (carried out by 23% of Internet users) and with home banking (47%); these two activities stand out as 'transactional', as they are similar to eCommerce and different from other types of activities [see fact sheet on eCommerce, "Transactional Activities, Table 5, on page 26"]. By this we are interested to know whether the use of specific transactions (by Internet users) correlate with use of credentials in daily life. We found that both have a positive relation with business-related credentials (the more credentials used, the more home banking and the more eGovernment activity), and with government entitlement cards [Table 65]. But both have a negative relation with the use of a national identity card. This may depend on high adoption of eGovernment and home banking in countries that do not issue identity cards to their citizens. To confirm this point, use of passports – which are indeed issued by governments – has a positive relation with both activities. Of course, this is also related with the different socio-demographic profile of people using different credentials – explored to a greater extent in the relevant section [4.3.2].

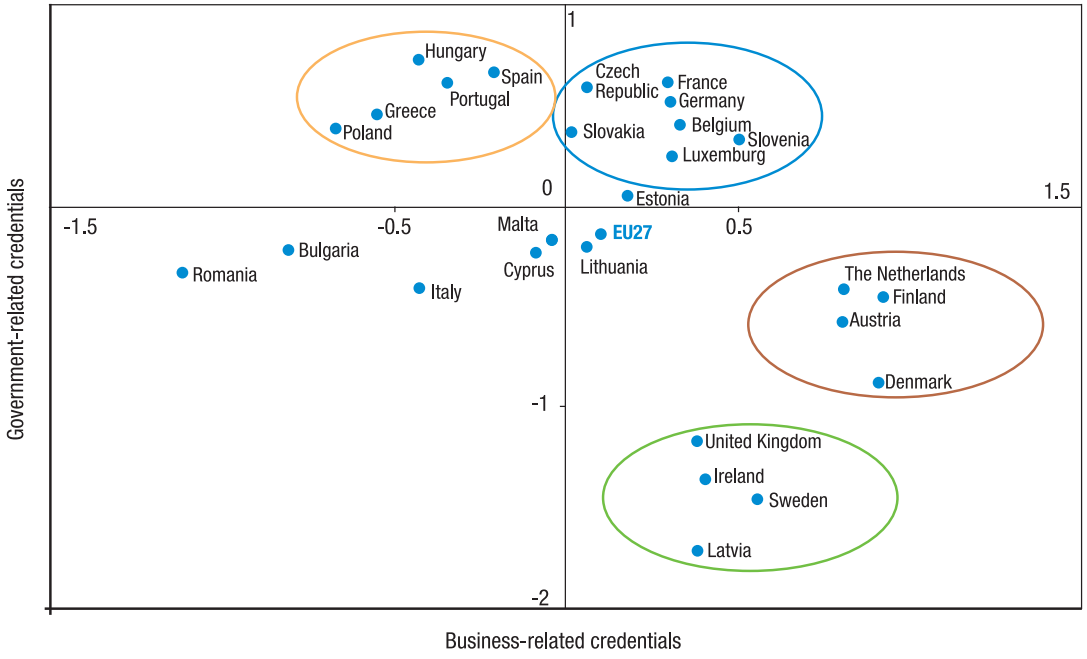
4.3.1 Use of credentials by country

Country analysis shows that credit cards and bank cards are used by vast majorities in Sweden (97%), the Netherlands (96%), Denmark (94%), and Finland (93%), but by fewer than half of respondents in Romania (43%), Greece (44%) and Poland (49%). In general, respondents from the north and the west of Europe are more likely to use credit cards and bank cards than those in eastern Member States.

In relation to this, we checked whether this depended on trust in the banking system rather than on country-specific cultural elements. Results of stepwise logistic regression [table not reported] indicate that trust alone makes only a little difference in the likelihood of having a bank/ credit card [+7% per each additional unit of trust, on a 1-4 scale]. Conversely, controlling for trust, country of residence makes a large difference [e.g. +21% for people living in Sweden, and -44% for residents of Greece]. Also, controlling for country and trust, we found that social position [+4% per additional point on 1-10 social scale] and younger age make more of a difference.

The use of national identity cards or residence permits varies greatly across countries. They are the most frequently used (of all eight types of personal credentials) in thirteen Member States, led by Bulgaria, the Czech Republic, Spain, Hungary (all 95%), Malta (93%) and Poland

Figure 18. Use of business-related credentials and government-related credentials by country



Base: EU27.
Source: QB14.

(92%). In contrast, they are scarcely used in Latvia (1%), Denmark (3%), the United Kingdom and Ireland (both 9%). Thus respondents from the east and south of the European Union are more likely to use national identity cards than those living in the north and west. Interestingly, there are no such differences in the use of passports.

Similarly, the use of government entitlement cards differs markedly across countries. They are widely used in Denmark, Slovenia (both 96%), the Czech Republic (94%), Hungary, Slovakia, Finland (each 93%), Belgium, Germany (92%) and Austria (91%), but rarely in Bulgaria (3%) and Romania (7%). This is hardly surprising since in latter countries, national identity cards are being widely used.

To simplify the view on this data, we examined country values for business-related and government-related credential use. By this, we are looking at what kind of credentials people are using in different countries [Figure 18]. Results show that differences are not necessarily regional or related to GDP and macro-economic indicators, but rather they respond to the structure of credentials in place in single countries.[58] In conjunction with what we noted above – that eGovernment is associated with increased use of business-related credentials - this fragmented structure may not bode well for the adoption of cross-border eGov services.

On the one hand, there are two groups of counties where use of government issued credentials is not very widespread: Latvia, Sweden, Ireland and the UK (marked in green); and Austria, Denmark, Finland and the Netherlands (marked in brown). Both groups include Member States whose citizens are slightly less likely to use government credentials and also more likely than people anywhere else to use business-related credentials (especially the second group). On the other hand, a number of Member States in 'continental' Europe (Belgium, Germany, France, Slovenia and Slovakia – marked in blue) significantly rely on both sets of

58 Stevens, T., Elliott, J., Hoikkanen, A., Lusoli, W., & Maghiros, I. (2010). The State of the Electronic Identity Market: Stakeholders, their Roles and Strategies (JRC Scientific and Technical Reports No. EUR 24567 EN). Sevilla: EC JRC Institute for Prospective Technological Studies.

Table 66. Use of credentials in countries by disclosure of different types of personal data in eCommerce

Country	Use of credentials		Disclosure		
			Biography information	Sensitive information	Security information
Belgium	Credit cards and bank cards	No	-.95	1.16	
		Yes	.09	-.13	
	National identity cards/ residence permit	No	-.24	.24	
		Yes	.14	-.18	
Austria	Credit cards and bank cards	No	-.66		-.30
		Yes	.13		.17
	National identity cards/ residence permit	No			.06
		Yes			.36
Germany	Credit cards and bank cards	No	-.54		
		Yes	.18		
	National identity cards/ residence permit	No	-.27		-.37
		Yes	.20		-.11
Spain	National identity cards/ residence permit	No			-.22
		Yes			.67
Sweden	National identity cards/ residence permit	No		-.28	
		Yes		-.08	
Poland	National identity cards/ residence permit	No	-.60	-.14	
		Yes	-.13	-.53	
Italy	Credit cards and bank cards	No	-1.73		-.21
		Yes	-.63		.32
Estonia	Credit cards and bank cards	No	-1.47		
		Yes	-.32		
United Kingdom	Credit cards and bank cards	No	-.33		
		Yes	.14		
Ireland	Credit cards and bank cards	No	-.16		
		Yes	.31		

Source: QB4b by QB14.

Base: eCommerce users.

Notes: Results reported are means of disclosure of type of information [derived from factor analysis].

Only significant differences in the two-sided test of equality for column means are reported (p< 0.01: there is a 99% probability that differences reported are not due to chance). Tests are adjusted for all pairwise comparisons within a column of each innermost subtable using the Bonferroni correction.

credentials – but do not use business-credentials as much as the group marked in brown. People in a fourth group of countries, namely Spain, Portugal, Hungary, Greece, and Poland (marked in orange) tend to rely to a great extent on government-related credentials. However, citizens of Romania and Bulgaria and also Italy tend to use slightly more government-related and slightly less business-related credentials, though they use fewer of either kind than citizens in the rest of Europe do.

Finally, there are also significant national differences in the relation between disclosure in eCommerce and use of credentials [Table 66]; in other words, what credential people use as they transact online. In some countries where the structure of electronic authentication

is most advanced [Austria, Belgium, Germany] people use government-related and business-related credential in relation to eCommerce disclosure. Again, the former credentials are usually associated with lower level of disclosure of sensitive information. In some countries, government related credentials are dominant [Spain, Sweden and Poland], while in some countries business credential underpin most of people's disclosure in eCommerce [UK, Ireland, Italy and Estonia]. These findings largely resound with industry-level analysis on the structure of the electronic identity market in Europe.[59]

4.3.2 Use of credentials by socio-economic status

Socio-demographic analysis yields some differences between groups in terms of gender, age, household composition, education, occupation, financial situation and social position [Figure 19]. This is true particularly for driving licenses, customer cards, passports and Internet accounts. Men are more likely than women to use these items – with the exception of customer cards and government entitlement cards. Respondents aged 15-24 are less likely

Figure 19: Use of credentials by socio-economic status

	Credit cards and bank cards	National identity cards/ residence permit	Government entitlement cards (e.g. BE : carte SIS, FR : carte VITAL)	Driving licence	Customer cards (loyalty cards, frequent flyer cards)	Passport	An account you use on the Internet (email, social networking, commercial services)	Student card
EU27	74%	68%	65%	63%	47%	43%	34%	5%
Sex								
Male	76%	68%	64%	72%	42%	45%	37%	6%
Female	72%	69%	66%	55%	51%	40%	31%	5%
Age								
15-24	63%	66%	54%	45%	36%	37%	52%	30%
25-39	84%	68%	64%	73%	53%	47%	47%	2%
40-54	81%	68%	69%	73%	52%	47%	36%	0%
55 +	66%	69%	69%	57%	42%	39%	16%	-
Respondent occupation scale								
Self-employed	83%	68%	64%	81%	51%	53%	39%	-
Managers	93%	61%	65%	83%	57%	66%	56%	-
Other white collars	87%	67%	64%	79%	58%	50%	46%	-
Manual workers	84%	69%	69%	74%	52%	43%	39%	-
House persons	59%	71%	60%	46%	47%	29%	20%	-
Unemployed	65%	71%	66%	50%	36%	33%	33%	-
Retired	64%	70%	69%	53%	40%	36%	14%	-
Students	57%	66%	50%	41%	33%	38%	54%	55%
Difficulties paying bills								
Most of the time	60%	71%	59%	49%	41%	27%	26%	4%
From time to time	70%	72%	62%	60%	46%	35%	30%	4%
Almost never	79%	66%	68%	68%	48%	49%	38%	5%
Self-positioning on the social staircase								
Low (1-4)	63%	76%	67%	50%	39%	29%	27%	4%
Medium (5-6)	76%	69%	66%	66%	48%	44%	35%	5%
High (7-10)	82%	60%	62%	72%	52%	56%	41%	7%

Source: QB14.
Base: EU27.

59 See report on the state of the electronic Identity Market, referenced in footnote 57.

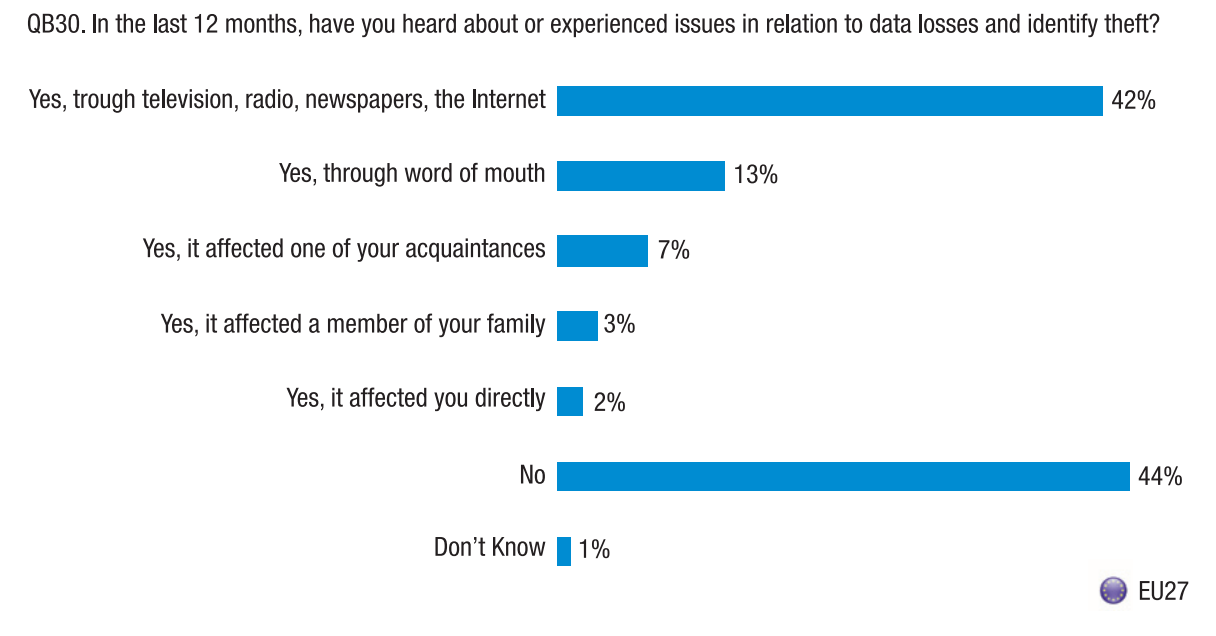
to have any of the items other than an internet account. Self-employed people, managers, other white collar workers and manual workers are the occupational groups most likely to have these items, with one exception: 54% of students have an Internet account. Furthermore, people who have difficulties with paying their bills and / or who place themselves low on the social scale are less likely to have leisure-related credentials – the latter group more often have national identity cards instead.

To further explore the nature of credentials, we examined the relative importance of the Internet in relation with the use of business- and government-related credentials. We used ordinary least square regression analysis to predict the use of credentials [table not reported]; results suggest that country, more than Internet access, matters for the use of government-issued credentials, controlling for other possible social determinants [e.g. age, affluence and gender]. Conversely, a combination of age, internet access, affluence and country predicts the use of business-related credentials. This may indicate that public institutions have a prominent role to play concerning the widespread adoption and use of credentials for government.

4.4 Awareness of identity theft and data loss

A question was included in the survey concerning the awareness of people of episodes of data loss and identity theft. The question aimed at gauging both the incidence of the phenomenon and the source origin of awareness, be it family discussion, social talk or derived from media information [Figure 20].[60] Overall, awareness of issues in relation to data losses and identity theft is widespread but not universal (58%); this awareness is mainly linked to news in the media (42% of all respondents); personal experience is marginal (2%). In more detail, few respondents

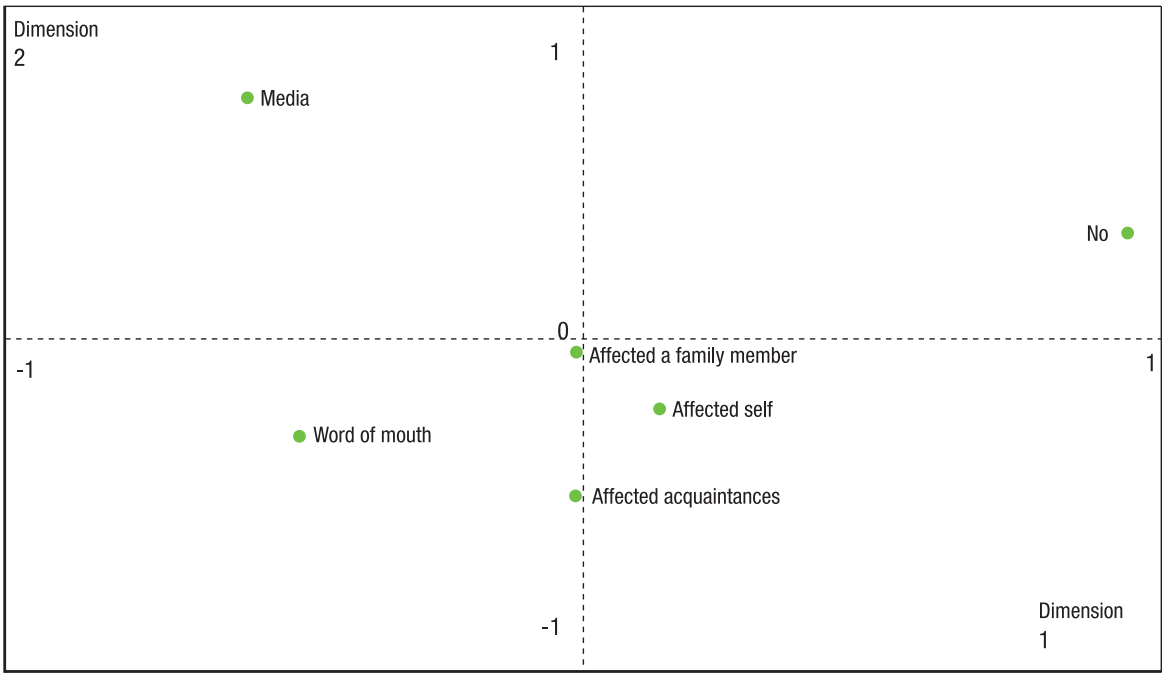
Figure 20. Awareness and experience of identity theft and data loss



Source: QB30.
Base: EU27.

60 QB30 In the last 12 months, have you heard about or experienced issues in relation to data losses and identity theft?

Figure 21. Dimensions of awareness and experience of identity theft and data loss



Source: QB30.
Base: EU27.
Note: Data is un-weighted.

experienced issues related to data losses and identity theft affecting their acquaintances (7%), a member of their family (3%), or themselves directly (2%). For the sake of comparison, identity theft only [but not data loss], affected about 3.5 % of US residents in 2010,[61] about double the EU figure.

The question was formulated in such as way as to elicit multiple responses; respondents could chose one or more sources of awareness, for instance reporting both media induced awareness and personal experience. Therefore, we conducted multi-dimensional scaling analysis of results, to see how different responses are related [Figure 21]. Unsurprisingly, 'No' responses stand alone, as the response is a clear opt-out. What is more interesting is that also media awareness stands alone, relatively unrelated to other responses; in other words, media awareness, as a category, do not imply any other type of encounter with identity theft and data loss. Outside these two, other items form a seeming continuum of proximity, ranging from the closeness of personal experience to the relative distance of word of mouth.

Looking at geographical differences [Figure 22], respondents are most likely to have heard of or experienced issues related to data loss or identity theft are in Latvia (74%), Sweden (73%), Ireland (72%), Denmark (71%), Finland (69%), and the UK (66%). This depends largely on media-related awareness and on a smaller degree on incidence of identity theft and data loss for self and family. Indeed, hearing through television, radio, newspapers and the Internet was by far most frequently mentioned in Latvia (69%), Sweden (62%), Denmark (61%) and Finland (59%) and the least in Portugal and Romania (both 22%). Hearing through by word of mouth happens most frequently in

61 Source: US representative sample of 5,004 adults via phone interview, conducted in November 2010. Javelin 2011 Identity Fraud Survey Report at: https://www.javelinstrategy.com/research/Brochure-209

Figure 22. Awareness and experience of identity theft and data loss by country

	Yes, through television, radio, newspapers, the Internet	Yes, through word of mouth	Yes, it affected one of your acquaintances	Yes, it affected a member of your family	Yes, it affected you directly
EU27	42%	13%	7%	3%	2%
BE	31%	9%	6%	3%	3%
BG	35%	15%	3%	1%	1%
CZ	53%	11%	5%	2%	1%
DK	61%	18%	7%	2%	3%
DE	51%	16%	6%	2%	2%
EE	53%	7%	4%	1%	2%
IE	55%	25%	8%	6%	3%
EL	43%	20%	12%	1%	1%
ES	50%	13%	6%	2%	1%
FR	44%	7%	5%	2%	3%
IT	25%	13%	11%	5%	1%
CY	50%	15%	8%	3%	2%
LV	69%	9%	4%	1%	2%
LT	26%	11%	4%	1%	2%
LU	50%	18%	10%	3%	4%
HU	36%	9%	10%	2%	1%
MT	25%	9%	5%	2%	2%
NL	45%	9%	5%	2%	3%
AT	35%	23%	11%	3%	1%
PL	36%	8%	3%	2%	1%
PT	22%	8%	5%	2%	1%
RO	22%	21%	4%	1%	1%
SI	49%	13%	3%	1%	1%
SK	44%	21%	8%	2%	1%
FI	59%	13%	5%	1%	1%
SE	62%	15%	14%	4%	5%
UK	49%	16%	8%	7%	5%

Highest percentage per country | *Lowest percentage per country*

Highest percentage per item | Lowest percentage per item

Source: QB30.
Base: EU27.

Ireland (25%) and Austria (23%). Experiences of issues related to data losses or identity theft affecting an acquaintance are most frequent in Sweden (14%), Greece (12%) and Italy and Austria (both 11%); those affecting a family member in the UK (7%), Ireland (6%), Italy (5%) and Sweden (4%); and those affecting respondents themselves in the UK and Sweden (both 5%) followed by Luxembourg (3%). It therefore appears that the awareness and experience of identity theft and data loss is heightened for specific reasons in the restricted score of countries reported, rather than being widespread across EU27.

We note that on the one hand media-related awareness for EU27 (42%) is already high, compared to for instance the share of total EU27 population that is involved in eCommerce (39%). However, it is does not seem to have any direct impact on lowering the incidence of either Identity theft or data loss.

Table 67. Awareness and experience of identity theft and data loss by socio-demographics

		Overall	Media	Self / family
	EU27	55%	42%	5%
Terminal education age	15-	44%	34%	4%
	16-19	55%	42%	5%
	20+	65%	52%	6%
	Still Studying	56%	37%	6%
	No full-time education	42%	26%	2%
Age	15-24	56%	39%	5%
	25-39	59%	44%	6%
	40-54	58%	45%	6%
	55+	49%	40%	4%
Occupation	Self-employed	59%	45%	6%
	Managers	68%	54%	7%
	Other white collars	61%	45%	7%
	Manual workers	56%	43%	5%
	House person	50%	39%	4%
	Unemployed	54%	40%	5%
	Retired	46%	38%	4%
	Students	56%	37%	6%

Source: QB30.

Base: EU27.

We then examined the socio-demographic traits of respondents who report no awareness, media awareness and personal and family awareness [Table 67].[62] First, overall awareness is far higher for formally educated people, in managerial and white collar positions, and in mid-life. It is far lower for older, retired people with lower levels of formal education. Second, media awareness if lowest for the older people described above, but also for students; again it is higher for people with university degrees and managers. Third, managers and other office workers and their families have been hit more frequently by identity theft and data loss; and again, retired people with lower levels of formal education have been less affected. Overall, results portray a clear social profile of people who are aware of and have been affected by identity theft and data loss.

We then examined the relation with Internet use and activities [Table 68]. Overall, Internet access makes a large and significant difference to awareness and experience of identity theft and data loss. Internet users are more likely to report overall awareness, media awareness and experience with the phenomenon. When people are online, different activities are associated with varying levels of awareness and incidence of identity theft and data loss. First, those that go online very often from different places are more likely to score higher on all three indicators. The relation between incidence of identity theft and data loss and number of activities conducted online is also strong [table not reported]. The incidence of identity theft is particularly high for people who are most time online and for their

62 Gender and marital status made very little difference to awareness of identity theft [not reported in the table].

Table 68. Awareness and experience of identity theft and data loss by Internet use

		Overall	Media	Self / family
	EU27	55%	42%	5%
Internet use and access index	No Internet	42%	32%	3%
	Low	56%	45%	5%
	Medium	**63%**	**48%**	**7%**
	High	**72%**	**54%**	**9%**
eCommerce	No	54%	40%	5%
	Yes	**67%**	**52%**	**7%**
Home banking	No	59%	43%	6%
	Yes	**65%**	**52%**	6%
Use of SNS & sharing sites	No	60%	48%	5%
	Yes	62%	47%	**7%**

Source: QB30 by D62, QB1a and QB1b.

Base: EU27 for Internet use and access index, Internet users for other variables.

families [three times higher than for non Internet users, 9% vs. 3%].

Second, about four in ten people who do not use the Internet are aware of identity theft and data loss; this is a lower than we expected for a phenomenon making the front page very often in most EU countries. It is certainly far lower than for people who actually use the Internet. The evidence reported in previous surveys conceding identity theft and data loss as an impediment to the uptake of the Internet may therefore be overstated.[63] Third, among internet users, people who do social networking and eCommerce appear to be more vulnerable to incidences of the phenomenon [7% vs. 5%]. Fourth, people doing eCommerce and home banking are very aware, both via the media and differently, of the issue of identity theft and data loss.

All in all, results confirm that identity theft and data loss are more of a reality online than offline; that the more people use the Internet, the more they become aware of the issue, but also that they become significantly more vulnerable to incidence; thus, general Internet skills alone do not provide and answer to identity theft and data loss [in a later section, we will examine the relation of incidence with specific data protection behaviours]; results also show that increased awareness, especially media awareness, may do little to mitigate incidence of negative experiences.

Finally, we crossed awareness and experience of identity theft and data loss with use of credentials, which were discussed above [Table 69]. We found three main results.

1 People with customer cards are more likely to have reported incidence of identity theft and data loss [6% vs. 4%]; the reverse is true for holders of national identity cards [4% of holders vs. vs. 8% of non-holders].

2 People who do not use credentials, especially bank and credit cards, are far less aware of identity theft and data loss via the media. Again, selective attention may explain this result.

3 People who use credentials, especially passports, are more aware of identity theft and data loss. People who travel may be particularly sensitive to the issue and to news related to it.

63 Related information (perception of concern from Eurostat Household survey data) as presented in Pillar 3, DAE scoreboard: http://ec.europa.eu/information_society/digital-agenda/scoreboard/docs/pillar/security.pdf

Table 69. Awareness and experience of identity theft and data loss by use of credentials

		Overall	Media	Self / family
Use of credit cards and bank cards	No	45%	29%	4%
	Yes	58%	46%	5%
Use of customer cards	No	50%	37%	4%
	Yes	60%	48%	6%
Use of national identity cards/ residence permit	No	58%	42%	**8%**
	Yes	53%	42%	**4%**
Use of passport	No	49%	36%	4%
	Yes	**63%**	50%	6%
Use of government entitlement cards	No	52%	36%	6%
	Yes	56%	45%	5%
Use of driving licence	No	49%	34%	5%
	Yes	58%	46%	5%

Source: BQ30 by QB14.

Base: EU27.

4.5 Identity protection behaviour, online and offline

Then, questions were asked directly regarding the way in which people protect their identity in their daily life and on the Internet.

4.5.1 Offline identity protection

A range of strategies are available to people to shield their identity from unwanted attention, from companies, largely, but also from fellow citizens and governments.[64] To protect their identity in daily life [Figure 23], a majority of Europeans give the minimum required information (62%) or do not disclose their bank details or PIN numbers (56%), while almost half disclose information only to people and organisations they trust (47%) or do not disclose their user names and passwords (45%). Overall, these numbers appear to us to be low, as significant minorities do not try to minimise disclosure, do no withhold bank details, provide information to controllers they do not trust and disclose usernames and passwords. As about 66% of people also use the Internet, the latter figure falls short of protecting everybody from prevalent internet crime such as phishing. All in all, this is in line with the widespread perception that disclosure is unavoidable in modern life [QB3, 74% of respondents see p.22 of EB-359 DP+eID report for correlations]. However, lack of protection is not caused by resignation: people who think disclosure is unavoidable are actually slightly more likely to protect themselves [r = .05 overall].

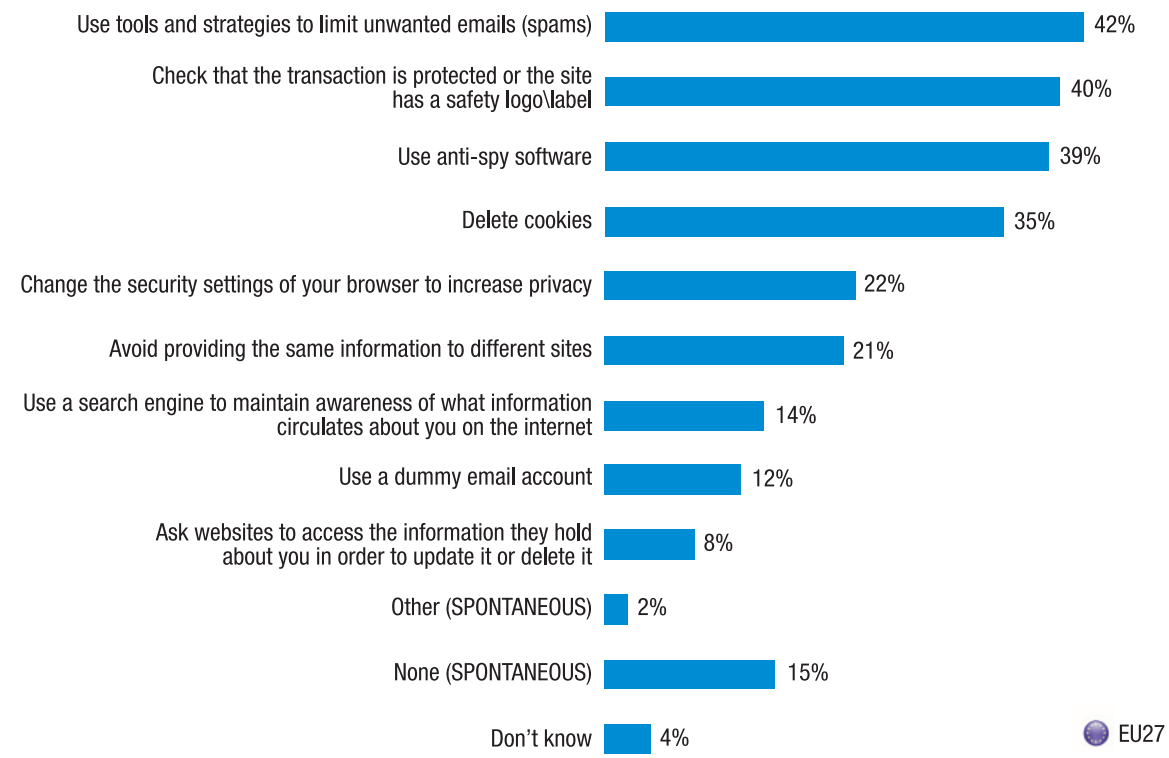
In relation to other specific behaviours, around three out of ten Europeans use cash instead of recorded transactions such as bank cards and transfers (30%), shred old bills, bank statements and the like (29%), do not disclose payment card details online (29%), and adjust the information they disclose to different contexts, for example depending on whether they are dealing with a company, a bank or a website (27%). Finally, only a few provide wrong information to protect their identity in daily life (7%).

Therefore, it seems that passive strategies, such as withholding personal information, occur more frequently than active strategies, such as deliberately providing wrong information or first evaluating the context and then adjusting the type of personal information disclosed. Factor analysis consolidates these results on identity protection behaviours, both for all respondents [Table 70]

64 QB15. In your daily life, what do you do to protect your identity? Please indicate all that apply in the following list.

Figure 23. Offline identity protection behaviours

QB16. And, specifically on the Internet, what do you do to protect your identity? Please indicate all that apply in the following list.



Source: QB15.
Base: EU27.

Table 70. Factor analysis of offline identity protection behaviours

	Factors		
	Minimise information	**Deception**	**Low tech actions**
Do not disclose your bank details or PIN numbers	.69		
Disclose information only to entities you trust	.64		
Give the minimum required information	.61		
Adjust the information you disclose to different contexts	.52	.40	
Provide wrong information		.94	
Use cash instead of recorded transactions			.90
Shred old bills	.44		.49
Eigenvalue	1.80	1.05	1.01
% Variance explained	25.8	15	14.6

Source: QB15.

Base: EU27.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0. 679; Bartlett's test of sphericity p=0.000; Convergence in 3 iterations; Minimum eigenvalue 1; Values below .03 are omitted.

and for Internet users [Table 71] (to be discussed further in section 4.5.3).

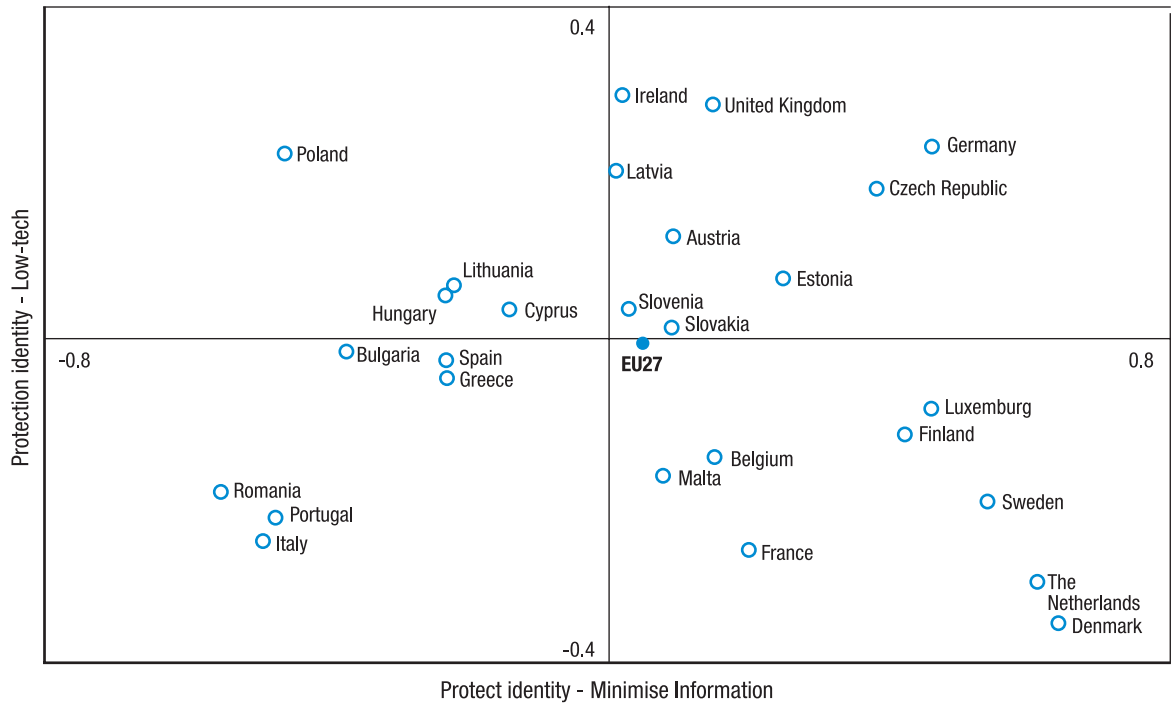
From the analysis of offline behaviours, it emerges that people use three identity protection strategies [Table 70]. First, they withhold disclosure in different ways, by keeping hold of some information, by minimising and by adjusting disclosure to context and recipient [minimisation]. A second strategy is one of outright deception, providing wrong information [deception]. A third strategy is composed of low-tech actions [rather than information management strategies], such as shredding bills and using cash [low tech].

4.5.2 Offline identity protection by country and socio-economic-status

First we will try to analyse the offline identity protection methods by country and then by socio-economic status [Figure 25]. In relation to comparison by country, there are marked differences among countries concerning the strategies adopted. In the Netherlands and in Scandinavian countries [Sweden, Denmark and Finland] a high percentage adopts various strategies to protect their identity in daily life. Identity protection is less common in southern European countries Portugal and Italy, the Baltic countries Lithuania and Latvia, and the eastern and central countries Poland, Hungary and Romania.

- Giving the minimum required information and not disclosing bank details or PIN number are the most common strategies in fourteen Member States; these two strategies stand in joint first place in two other countries, Denmark (78%) and in the UK (66%). But significant differences exist between countries. For instance, over three-quarters of respondents in Finland (78%), Luxembourg (76%), and Germany and the Netherlands (each 74%) give the minimum required information, whereas half or under

Figure 24. Minimisation vs. low-tech protection behaviours by country



Source: QB15.
Base: EU27.

do so in Poland (45%), Lithuania and Italy (both 50%).

- While large majorities in Sweden (85%) and the Netherlands (84%) do not disclose their bank details or PIN numbers, around a third or less do so in Italy (27%), Poland (34%) and Romania (35%). This is mirrored by not disclosing user names and passwords: around three-quarters of respondents in Sweden (78%), Finland (77%) and the Netherlands (73%) adopt this strategy compared to only 14% in Italy and 16% in Bulgaria.

- Respondents use cash instead of recorded transactions (such as bank cards and transfers) as a strategy to protect their identity most often in Poland (44%), Austria (40%), Hungary (39%) and Latvia (38%) and least often in the Netherlands (15%), Finland (17%), France and Denmark (both 18%). Interestingly, this strategy reverses the order of countries found in respect of all other strategies. However, it is consistent with the enhanced use of the Internet in these countries which disallows low-tech protection behaviour.

Again, it is interesting to see graphically [Figure 24] how different countries fare in relation to each other on these traditional behavioural actions to protect one's identity use of cash [low tech] vs. relatively recent, information based strategies [minimise]. In Sweden, Finland, Denmark and the Netherlands people tend to minimise information and not to engage in low-tech behaviours, possibly due to the digital nature of most transactions. In countries such as Germany and the Czech Republic people tend to be active on both fronts. As it was noted, in southern and eastern countries, people tend to score low on both counts. This may be explained as follows: offline strategies are linked to concerns about observation, while minimisation is linked to Internet use, especially eCommerce. People in Nordic countries are generally less concerned about their behaviour being recorded, and are more likely to use eCommerce. The situation is inverse for countries in the bottom-left quadrant of Figure 24.

A socio-demographic breakdown reveals great disparities between groups in respect of all the strategies to protect identity in daily life, as age, education and occupation make a difference [Figure 25]. With respect to all but two strategies, the longer respondents have spent in education, the more likely they are to actively protect their identity; the two exceptions are the use of cash instead of recorded transactions and shredding old bills and the like. This reflect the relatively simple fact that people with higher education, and younger as a result, are more likely to be part of the digital economy, rather than of the paper-based economy.

Turning to occupation, managers and other white collar workers are more likely to use each of these strategies (apart from the use of cash instead of recorded transactions), whereas students tend to use most of the strategies less with the exception of not disclosing their user names and passwords (53%) and providing wrong information (11%). Overall, therefore, identity protection is more developed in mid-life, as it may be natural, because people engage in a range of financial and social transaction around this phase of life. Finally, the level and nature of Internet use has an impact on results. For instance, 66% of online shoppers do not disclose their user names and passwords compared with 50% of those who do not shop online. Again, 70% of online shoppers do not disclose their bank details or PIN numbers, compared with only 55% of other Internet users.

Figure 25. Offline identity protection by socio-economic traits

QB15 In your daily life, what do you do to protect your identity? Please indicate all that apply in the following list. (MULTIPLE ANSWERS POSSIBLE)

	Give the minimum required information	Do not disclose your bank details or PIN numbers	Disclose information only to people/ organisations you trust	Do not disclose your user names and passwords	Use cash instead of recorded transactions (bank cards, transfers)	Shred old bills, bank statements, credit card receipts, etc.	Do not disclose payment card details online	Adjust the information you disclose to different contexts (e.g., depending on whether you are dealing with a company, a bank or a website)	Provide wrong information
EU27	62%	56%	47%	45%	30%	29%	29%	27%	7%
Age									
15-24	62%	52%	45%	51%	25%	17%	27%	25%	10%
25-39	65%	60%	47%	51%	25%	29%	32%	31%	9%
40-54	65%	61%	48%	50%	28%	30%	34%	31%	7%
55 +	59%	51%	46%	34%	37%	33%	25%	23%	4%
Education (End of)									
15-	54%	44%	41%	25%	38%	29%	19%	17%	5%
16-19	62%	58%	47%	45%	30%	31%	32%	26%	7%
20+	71%	69%	53%	61%	23%	32%	36%	39%	8%
Still studying	63%	50%	46%	53%	25%	15%	26%	28%	11%
Respondent occupation scale									
Self-employed	65%	59%	50%	49%	26%	26%	32%	36%	7%
Managers	76%	73%	54%	69%	19%	36%	39%	43%	9%
Other white collars	66%	63%	49%	55%	22%	30%	36%	33%	9%
Manual workers	63%	60%	47%	47%	28%	30%	32%	26%	7%
House persons	60%	44%	42%	32%	37%	25%	21%	20%	5%
Unemployed	59%	50%	42%	42%	34%	26%	28%	23%	7%
Retired	56%	51%	45%	31%	37%	33%	24%	21%	4%
Students	63%	50%	46%	53%	25%	15%	26%	28%	11%

Source: QB15.

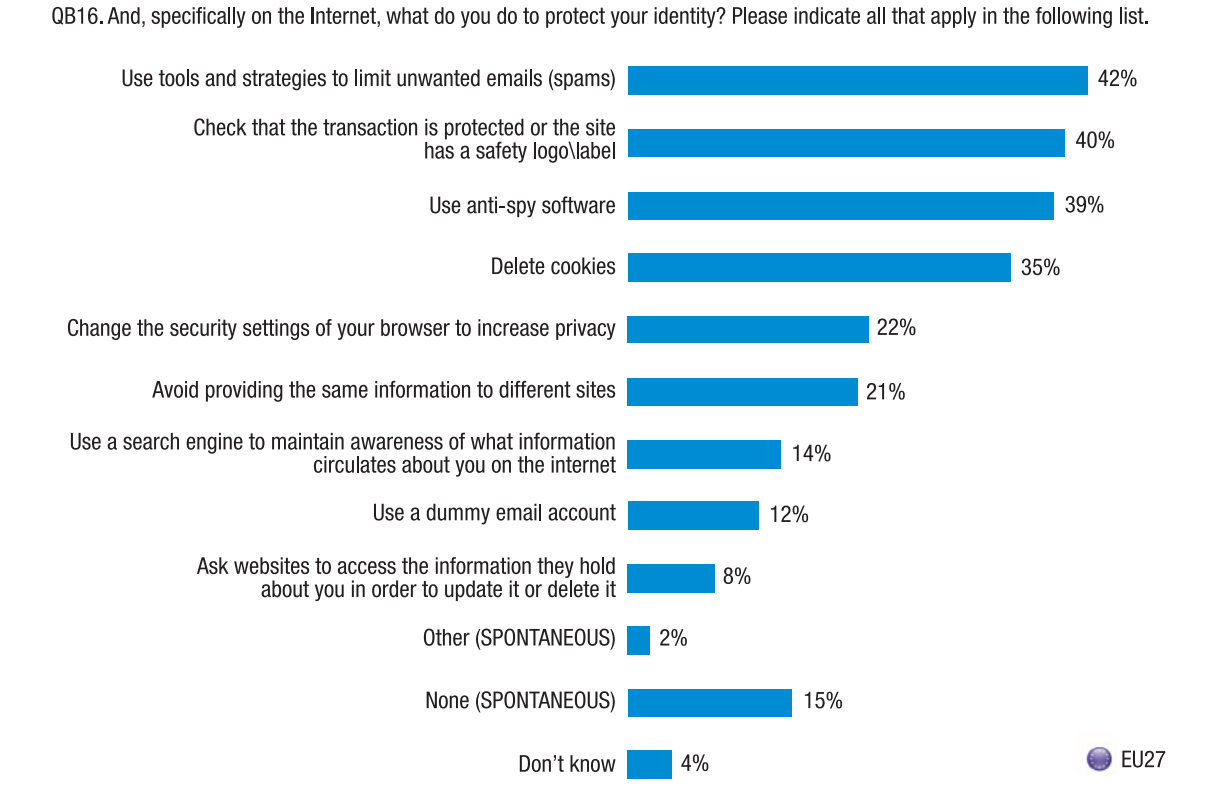
Base: EU27.

4.5.3 Online identity protection

We then looked at the same question for Internet users only. But an additional question was asked only of Internet users, which gauged the extent to which users adopted a range of Internet-specific behaviours intended to protect their personal identity data online.[65] The main result is that online self-protection is not widespread [Figure 26]. Only four in ten European Internet users apply tools and strategies to limit unwanted emails (spam) (42%), check that a transaction is protected or that the site has a safety logo or label (40%), or use anti-spy software (39%). One-third of respondents delete cookies (35%). A sizeable minority of 15% spontaneously say that they do nothing to protect their identity on the Internet.

With the additional responses that made sense online, such as not disclosing user names and passwords, and not disclosing payment card details online, we found overlapping though slightly different results: namely four sets of overall identity protection behaviours rather than three. As for non Internet users, factor analysis [Table 71] found minimisation, low-tech and deception behaviours, very similar to what we described above. Additionally, Internet users adopt a number of security-enhancing withholding behaviours, such as not disclosing username and passwords and not disclosing payment card details online. Interestingly, withholding bank details or PIN numbers now belongs to this group of behaviour, rather than to

Figure 26. Online identity protection behaviours [Internet users]



Source: QB16.
Base: Internet users (66% of total sample).

65 QB16: And, specifically on the Internet, what do you do to protect your identity? Please indicate all that apply in the following list.

Table 71. Factor analysis of identity protection behaviours [Internet users]

	Factors			
	Withhold	**Minimise**	**Low tech**	**Deception**
Do not disclose user names and passwords	.83			
Do not disclose bank details or PIN numbers	.82			
Do not disclose payment card details online	.69			
Give the minimum required information		.70		
Disclose information only to entities you trust		.69		
Adjust the information you disclose to different contexts		.60		
Use cash instead of recorded transactions			.91	
Shred old bills			.48	
Provide wrong information				.95
Eigenvalue	2,37	1,16	1,10	,97
% Variance explained	26	12,5	12	11

Source: QB16.

Base: Internet users.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0.723; Bartlett's test of sphericity p=0.000; Convergence in 5 iterations; Minimum eigenvalue .975; Values below .04 are omitted.

minimisation behaviours as for the entire sample. This protective behaviour appears to be required in an online environment where risks of identity theft and fraud are especially felt [especially identity theft and fraud for eCommerce and SNS, and observation for financial transactions for everyday life activities; see EB-359 on these points]. Overall, this confirms the intuitive idea that being on the Internet requires more sophisticated strategies of self protection than those one has to implement in offline, everyday life.

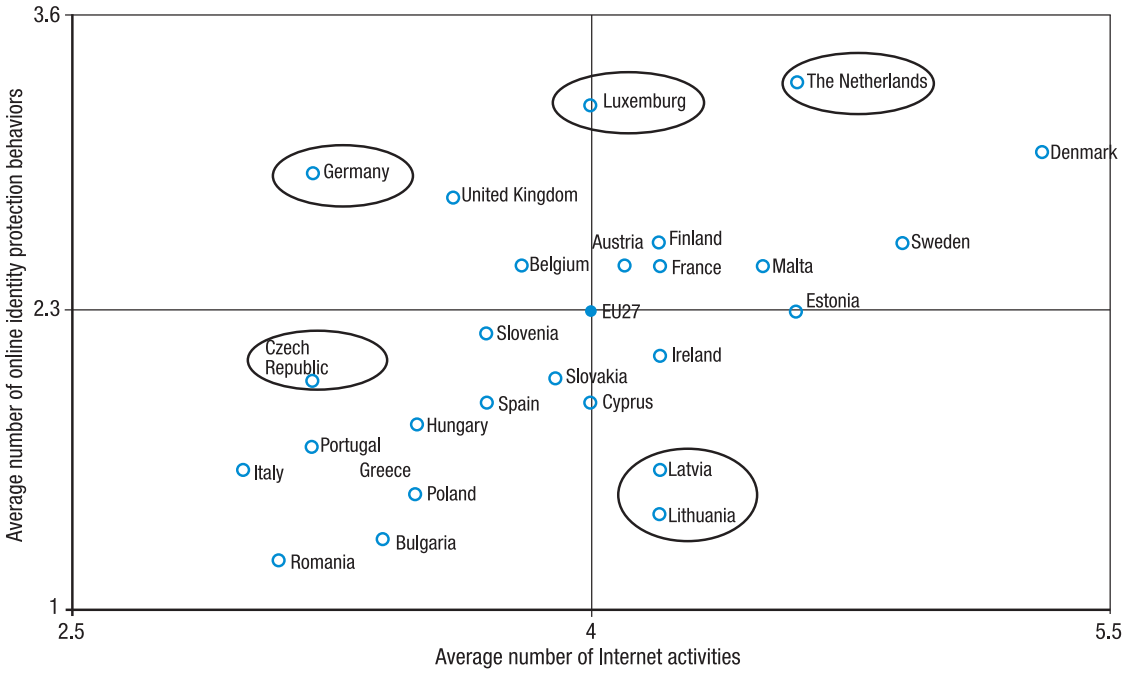
Largely, protection behaviour rests on passive use of existing tools rather than on active strategies of information control. This may also imply that where these tools are not available, or are cumbersome to use for the average user, people are unlikely to take proper care of their personal identity data online.

4.5.4 Online identity protection by country and socio-economic-status

In terms of countries [table not included EB-359, QB16 by country, p.109], the Netherlands, Luxembourg and Denmark stand out as Member States with the largest numbers of Internet users who use a variety of strategies to protect their identity on the Internet. This habit is least common in the Baltic countries Lithuania and Latvia, and the eastern EU Member States Romania and Bulgaria. Again, there is variance within this general figure [Figure 27]. In other words, people in some countries tend to stand more protected online regardless of the number of activities they carry out on the Internet (i.e. The Netherlands, Luxembourg); while people in Latvia and Lithuania tend to protect themselves partially despite higher than EU27 average Internet use. Such deviations from the trend hint at the importance of variables others than Internet use to explain protection; these may have to do with national technical culture, with national attitudes concerning observation and with maturity of the market for online protection tools.

As far as socio-economic status is concerned, higher education and occupation as a professional make a difference for higher identity protection on the Internet; whereas

Figure 27. Internet protection behaviours in relation with Internet activities



Source: QB16 by QB1b.
Base: Internet users (66% of total sample).

gender and age make smaller differences [table not included EB-359, QB16, p. 111]. A general pattern emerges in which the more technical or procedural (top five) strategies are more likely among men than women, among older respondents than the youngest (15-24), among respondents who spent longer in education than less educated interviewees and among managers than those unemployed.

However, the largest differences exist between groups with different Internet skills: active Internet users (++) are more likely than less active users (--) to apply each of the strategies. Practically the only strategy less active users (--) use almost as much as more active users (++) is to avoid providing the same information to different websites. There is a strong and significant correlation [r = .44] between the overall number of internet activities carried out [a proxy for internet skills], and online protection behaviour. In other words, those who are more active online also protect themselves more; this is good news, as Internet skills thus measured are related to years spent online [thus benefiting older users] and to young age [thus benefiting younger users]. This correlation is slightly weaker if we do not consider eCommerce activities [r = .41]. Indeed, more than half of online shoppers check that the transaction is protected or that the site has a safety logo/ label (52%), use tools and strategies to limit unwanted emails (spam) (52%) and use anti-spy software. Indeed, this is not surprising as they have more to lose and are more cautious than SNS users.

Finally, we looked jointly at questions of online and offline identity protection for Internet users. To identify commonalties and differences, we conducted factor analysis of the two questions jointly. The underlying assumption originated above: people seem to be more careful in protecting their personal data on the Internet than offline. The analysis found that European Internet users use six strategies to protect their personal identity data [Table 72]. Four are strategies described above as common to online and offline: minimisation, withhold, low-tech and deception. Additionally, the analysis found two strategies that we labelled

Table 72. Factor analysis of online identity protection behaviours

	Reactive	Withhold	Minimise	Proactive	Deception	Low-tech
Use anti-spy software	.76					
Delete cookies	.73					
Use tools and strategies to limit unwanted emails	.58					
Check that the transaction is protected	.43					
Do not disclose your bank details or PIN numbers		.81				
Do not disclose your user names and passwords		.80				
Do not disclose payment card details online		.70				
Disclose information only to entities you trust			.68			
Adjust the information you disclose to different contexts			.62			
Give the minimum required information			.59			
Ask websites to access the information they hold on you				.72		
Use a search engine to maintain awareness				.64		
Change the security settings of your browser				.49		
Avoid providing the same information to different sites				.43		
Provide wrong information					.78	
Use a dummy email account					.75	
Use cash instead of recorded transactions (bank ca						.82
Shred old bills						.51
Eigenvalue	3.46	1.57	1.31	1.08	1.03	1.03
% Variance explained	19%	9%	7%	6%	6%	6%

Source: QB15 and QB16.

Base: Internet users.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0.81; Bartlett's test of sphericity p=0.000; Convergence in 6 iterations; Minimum eigenvalue .975; Values below .04 are omitted.

reactive and proactive. The former includes software-based protective behaviours such as using anti-spy software, deleting cookies, and checking for SSL connection. The latter includes activities that require higher user initiative, such as use of search engines to maintain awareness and asking websites to access the information they hold on them.

4.5.5 Offline and online identity protection, credentials and identity theft

Then, we wished to examine the relation between the extent to which people protect themselves in daily life, and the use of credentials, on the one hand; and the experience and awareness of identity theft and data loss

on the other [Table 73]. We found a number of interesting results:

1 Those who are not aware of identity theft and data loss are less likely to protect themselves, online and offline, especially this is true for minimisation of personal data disclosed and use of protecting software. Media awareness is particularly important to make people minimise personal data disclosure [r = .20].

2 People who use business-related credentials are much more likely to try to minimise the information they disclose [r = .44]; Internet users are more likely to withhold information and to use software to protect themselves. However, they are no more likely to engage in active strategies of identity protection.

3 People who use government-related credentials are also more likely to minimise information, though to a lesser degree [r = .08]; but those who use the Internet are more likely to use proactive rather than reactive strategies of identity protection behaviour.

4 Those whose family or themselves have suffered identity theft and data loss appear to be more likely to use deception behaviour [r = .08]; and to use reactive and proactive internet strategies to protect their personal data.

Table 73. Offline identity protection by use of credentials and identity theft

		Business -related	Government -related	No awareness	Media awareness	Self-family incidence
All users	Minimise	**.44**	.08	-.16	**.20**	
	Deception	.05		-.10	.04	.08
	Low-tech	-.05		-.05	.06	
Internet users	Withhold	**.25**	.09	-.04	.11	
	Reactive	**.23**	-.06	-.13	.12	.07
	Proactive		.07	-.05		.05

Source: QB15 by D62.

Base: EU27 and Internet users, respectively.

Note: As the sample is large, only significant relations at p < 0.001 are reported [i.e. when there is a 99.9% probability that the relation reported is not due to chance].

Results reported are:

1. Pearson's correlation coefficient for pairs of factors and/or scales.

2. Point-biserial correlation for factors and/or scales crossed by values.

4.6 Relations with other variables

In this section, we examine use of credentials, awareness and experience of identity theft and protection of personal data in relation to other relevant variables [Table 74].

Use of credentials in Europe

Overall, use of business-related credentials, more than use of government-related credential, is intertwined with people's attitudes concerning data protection:

- For Internet users, use of business-related credentials is strongly associated with online transactions such as home banking, eGovernment and ecommerce [r = .39]; but it is inversely related with online social activities [r = -.11]. This is related to life-cycle, as reported above. Internet behaviour is unrelated to the use of government-related credentials.

- Those who use credentials of both types are more likely to trust institutions as data controllers, especially business-related credentials [r = .13]; those who do not trust companies as data controllers are likely to make greater use of government-related credentials [r = -.12]. Therefore, use of credentials may be enhanced by portability of trust from public institutions to commercial institutions, via the greater use of government-supported, if not issued outright, credentials, or by PPPs.

- Those who use business-related credentials are less concerned about being observed in their everyday life [CCTV, mobile, transactions], but when they use the Internet they are uncomfortable with online profiling [r = -.10] and concerned about use of personal data for other aims that the original [r = .09].

- Concerning regulation, users of business-related credential are strongly in favour of homogeneous data protection right across EU [r = .19], to be informed when their personal data is lost or stolen [r = .17], and to be able to edit/delete they data whenever they wish so [r = .11]. But they are as keen to be able to move their data between providers [portability] than people who do not use credentials, or do not use them as much [figure not reported in Table 74]. It appears that remedies requiring more of people's initiative are less popular than institution-centred remedies.

Awareness of identity theft and data loss

Media awareness emerged from the analysis as the most significant variable in relation to other opinions expressed by respondents. These are reported below and in the table. Results for 'no awareness' are largely symmetrical to results for 'media awareness'. Results for actual personal and family incidence of identity theft and data loss do not correlate significantly with any other data protection opinions and behaviours, except for advanced software use of internet users [r = .08]. Both these sets of results have been omitted.

- Media awareness of identity theft is heightened for people who use the internet to carry out transactions [r = .14], it is not any higher for people engaging in social activities. Identity theft and data loss may thus be associated in people's minds to financial rather than to social damage [this confirms results reported in the fact sheet on eCommerce].

- Those who do not trust companies to protect their data, and those who are not very happy disclosing data are slightly more likely to have heard about the phenomenon in the media.

- For Internet users, media awareness is related to higher concern of reuse of personal data for other purposes [r = .11], and to the impressions that at some point they had to over-disclose personal data [r = .08]. The media appears to compound one's own experience of over-disclosure.

- Concerning remedies, media awareness appears intertwined with calls for enhanced regulation, including greater harmonisation of data protection rights across EU27 [r = .15], request for information if/when data lost or stolen [r = .12] and the possibility to delete personal data [r = .12].

Identity protection behaviour, online and offline

Overall, online and offline personal data protection behaviours are strongly associated with overall attitudes towards disclosure, with trust in data controllers [or lack thereof], and with online activities for Internet users. Specifically, data minimisation strategies and what we term reactive online strategies, based on the use of available software, appear to determine and

be determined by people's perceptions and regulatory preferences concerning personal data:

- People doing different things on the internet have significantly different ways of staying protected online [or not]. Internet users engaging in online transactions are much more likely than ordinary internet users to take a range of measure to protect their data online, including data minimisation [r = .30], reactive software use [r = .36] and to withhold sensitive information [r = .13]. People with advanced internet skills tend to use proactive [r = .19], reactive [r = .16] and deception [r = .15 !] strategies rather than traditional protection measures. Conversely, people engaging on social activities are less likely to minimise and withhold, but more likely to use proactive personal data management strategies [r = .16].

- Attitudes towards personal data disclosure in general matter greatly for the protection of one's data. Specifically, those who are happy disclosing personal data are much less likely to minimise data [r = -.19], as may be obvious, but are also less likely to withhold sensitive information [r = -.16] and to use software measures to protect their data [r = -.07]. Same results emerged for people who are comfortable with online profiling [respectively r = -17 and r = -.12]. Conversely, those who see disclosure as unavoidable try to protect themselves in a range of ways, especially with software [r = .14]. Interestingly, high levels of concern about observation seems to engender more practical responses, including low-tech behaviours [r = .08] and proactive data management online [r = .05].

- Trust in institutions as data controllers seems to be associated with higher levels of self-protection, apart from deception. On the contrary, those who trust companies tend to be less active protecting themselves across the board, but especially they are less likely to minimise information they disclose [r = -.12], and to withhold sensitive information [r = -.10].

- All in all, existing rules and principles of data protection appear to engender virtuous responses on the part of internet users regarding self-protection. Namely, those who think they had to disclose more that they wished actually did so [minimisation r = -06, withholding r = -11], but may have compensated by using reactive, proactive and deception strategies [r =~ .10 for the three]. Information about data collection conditions is associated positively with reactive and proactive behaviour, and with minimisation. Finally, concern about re-use of one's data is associated with significant minimisation of the data disclosed [r = .15].

- Data minimisation appears to be strongly correlated with issues of regulation. In other short, peoples who minimise the information they disclose also tend to have particularly strong feeling regarding the needs for stronger protection of their rights in EU27 [r = .20] and enhanced control of their personal data, such as deletion on demand [r = .17] and data breach notification [r = .21].

Table 74. Correlations between identity-related variables and other relevant variables

Variables			Use of credentials		Awareness of identity theft and data loss	Offline identity protection			Online identity protection		
Measurement			2 Factors		1 Value	3 Factors			3 Factors		
		Values	Business-related	Govt-related	Media awareness	Minimise	Deception	Low-tech	Withhold	Reactive	Proactive
Internet activities	3 Factors	Social internet	-.11			-.07	.04	-.09	-.08	.11	.16
		Transactions	.39		.14	.30	.08	-.06	.13	.36	.08
		Advanced				.05	.15			.16	.19
Attitudes towards disclosure	2 Factors	Unavoidability	.09		.08	.06	.05	.05		.14	.04
		Propensity	-.05	-.05	-.06	-.19	-.04	-.11	-.16	-.07	
Trust	2 Factors	Trust in institutions	.13	.04		.13	-.05	-.07	.04	.04	
		Trust in companies	-.04	-.12	-.06	-.12	-.04	-.07	-.10	-.06	
Concern about observation	1 Factor		-.08	.04			.04	.08			.05
Comfort with online profiling	4-point scale		-.10	-.08	-.06	-.17		-.05	-.12		
Informed about data collection conditions	4-points scale		.06		.06	.07				.14	.09
Required to over-disclose	4-points scale				.08	-.06	.11		-.11	.08	.11
Concern about reuse	4-point scale		.09		.11	.15		.12	.08	.05	
Importance of same data protection right across EU	4-point scale		.19		.15	.20		.04	.11	.13	
Desire info if/when data lost or stolen	4-point scale		.17	.04	.12	.21	-.04		.12	.05	
Possibility to delete personal data	1 Value	Whenever one wants	.11	.10	.12	.17			.12	.07	

As the sample is large, only significant relations at p < 0.001 are reported [i.e. when there is a 99.9% probability that the relation reported is not due to chance].

Results reported are:

1. Pearson's correlation coefficient for pairs of factors and/or scales.

2. Point-biserial correlation for factors and/or scales crossed by values.

3. Phi for relations between values, when they can be considered as multiple categorical (e.g. colour: white, red, or green).

Note: For 'Attitudes towards disclosure': factors extracted for Internet users only are used.

Table 75. Relevant samples for correlations

	N for all questions	N for online identity protection, if different
Social internet	17,520	
Online transactions		
Software activities		
[all] Disclosure is unavoidable	22,269	
[all] Disclose happily		
[internet users] Disclosure is unavoidable	15,306	
[internet users] Disclose happily		
Overall concern about observation	23,021	16,499
Informed about data collection conditions when disclosing personal data to access a service	14,293	
Comfort with online profiling	16,283	
Required to provide more personal information than necessary for online services	16,769	
Trust in institutions	20,452	15,581
Trust in companies		
Concern about unannounced re-use of personal data for different purpose than original	25,794	17,265
Desire to be informed by controller whenever personal data held is lost or stolen	25,617	17,121
Possibility to delete of personal data held by controllers: Whenever you decide to delete it	17,520	
Importance of having same data protection right across Europe	25,649	17,228
Perceived effectiveness of DPO to protect personal data in large companies	24,070	16,546
Knowledge about national data protection authority	25,596	16,959

5 FACT SHEET: Medical Information as Personal Data in Europe

5.1 Question context

The questionnaire included several questions regarding health related information as personal information in the context of social computing,[66] namely:

5.2 Legal context

The main legal instruments related to medical information are the following:

Table 76. Survey questions relevant to health related information

Question code	Shorthand	Formulation	Rationale
QB2	Data considered as personal	Which of the following types of information and data that are related to you do you consider as personal?	To explore the perception of medical information as personal information.
Social Networking Sites and sharing sites			
QB4a	Personal data disclosure	Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?	To gauge the extent of disclosure of different types of personal data; this question follows on a previous questions asked of all respondents regarding what information they though was personal assess.
QB5a	Reasons why disclose	What are the most important reasons why you disclose such information on social networking sites and\ or sharing sites?	To assess the reasons why people disclose personal data in SNS, whether for leisure, to get better offers, to save time, etc.
QB6a	Control on information disclosed	How much control do you feel you have over the information you have disclosed on social networking sites and\ or sharing sites, e.g. the ability to change, delete or correct this information?	To determine the level of perceived control on the data disclosed in SNS. This is related both to the right of access to one's information and to the capacity of people to actually control their data once they have disclosed it.
QB7a	Risks related to disclosure	I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information on social networking sites and\ or sharing sites?	To explore the risks people associate with the disclosure of personal data in SNS. Several risks may be associated with disclosure, including risks to reputation, to personal safety, to data integrity, etc… .
QB25	Trust in different institutions	Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information. To what extent do you trust the following institutions to protect your personal information?	To explore the level of trust that people bestow different institutions with, among which medical institutions, to protect their personal data.

66 Just 3% of ecommerce users stated that they have disclosed medical information in this context. Due to this small figure we have carried out the analysis in the context of Social Computing (disclosure is 5%).

- Data Protection Directive (95/46/EC). This directive is the general EU law in the field of protection of personal data and the most prominent legislative act regulating the processing of medical data. Its objective is to protect the privacy of individuals while enabling the free flow of personal data within the EU in the context of the internal market. It lays down obligations on data controllers and specifies the rights of data subjects. The directive provides special protection for personal data related to health,[67] prohibiting in principle its processing. Limited exemptions to this prohibition principle are foreseen in the Directive, in particular if processing is required for specified medical and healthcare purposes, if the data are processed by a health professional subject to an equivalent obligation of secrecy.

- The results presented in this fact sheet depict EU citizens' perceptions, attitudes and behaviours regarding the disclosure of medical information. These results may prove useful to the current revision of the data protection directive, namely regarding the need to introduce stricter rules and/or to harmonise the requirements to obtain, administer and comply with the requisite of prior informed consent for the processing of personal data for health purposes. The results obtained regarding the citizen's views on genetic data may also be linked to another important theme of the current data protection revision, that is, the question of whether "genetic data" should be considered as a separate new category in the list of categories of "sensitive data."

- ePrivacy Directive: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. This directive particularises and complements the Data protection directive with respect to the processing of personal data in the electronic communications services over public communications networks to ensure confidentiality of communications and security of networks, including an obligation to notify personal breaches to the competent authority at national level. This directive is relevant and applicable in the case of disclosure of medical information in the online environment, such as in social computing sites, social networking sites, etc.

- Directive 98/48/EC of the European parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. This Directive provides the definition of information society services (Art.1(2)) which applies to social networking and eCommerce sites.

- Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997). This recommendation explicitly defines the expression "medical data" ("which refers to all personal data concerning the health of the individual. It refers also to data which have a clear and close link with health as well as to genetic data"), and the expression "genetic data" ("which refers to all data, of whatever type, concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals"). It is important

67 According to the European Court of Justice, the expression 'data concerning health' used in Article 8(1) should be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual. By way of example: reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of the directive. European Court of Justice, Judgement of 6 November 2003, Case C-101?01 – Bodil Lindqvist, 50, 51.

to bear in mind these definitions when analysing the citizens' own perceptions regarding the concepts of health data and genetic data.

- Directive on Patients' Rights in Cross-Border Healthcare: Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. The directive applies to individual patients who decide to seek healthcare in a Member State other than the Member State of affiliation. By following its provisions, Member States must ensure that the healthcare providers on their territory apply the same scale of fees for healthcare for patients from other Member States, as for domestic patients in a comparable medical situation (Art. 4, para.4). Taking into account that the majority of EU citizen wishes to benefit from the same protection over their personal information regardless of the EU country in which its is collected and processed, the results observed in this fact sheet seem to be in line with this very recently adopted directive, which contributes to the harmonization of the access to healthcare within the EU (Member States must adopt the necessary laws, regulations and administrative provisions to implement this directive by 25 October 2013).

- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "A Digital Agenda for Europe."

- The overall desire to have the same level of data protection across the EU, the general trend to qualify medical information as sensitive and the attitude towards its non-disclosure render particularly important and necessary the key actions planned by the European Commission in the field of eHealth:

  - **Key Action 13:** *Undertake pilot actions to equip Europeans with secure online access to their medical health data by 2015 and to achieve by 2020 widespread deployment of telemedicine services.*

  - **Key Action 14:** *Propose a recommendation defining a minimum common set of patient data for interoperability of patient records to be accessed or exchanged electronically across Member States by 2012.*

  The results verified in this fact sheet reinforce the understanding that EU citizens may only be able to enjoy the same degree of protection of their medical information, qualified as sensitive data, across different EU Member States if secure online access systems to one's medical data are implemented and interoperability standards of electronic exchange of patients records are established.

Other legal sources concerning medical information from a data protection point of view are the following:

- Article 8 of the European Convention of Human Rights (ECHR).

- Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

- Convention n.108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted on 28 January 1981.

- Convention n.164 for the protection of Human Rights and dignity of the human being with regard to the application of biology and medicine: Convention on Human Rights and Biomedicine and its Additional Protocols.

For details regarding the methodology used in the survey, please refer to the main report

[Special Eurobarometer 359: "Attitudes on Data Protection and Electronic Identity in the European Union"]. Some of the question in the survey we asked both of social networking site users and of people suing online sharing sites. In this fact sheet, we examine the responses – behaviours, attitudes - of social networking users.

5.3 Medical information as personal data

All respondents were asked what information they consider to be personal [Table 77]. Around three-quarters of Europeans think that the following are personal: financial information, such as salary, bank details and credit record (75%), **medical information such as patient records, health information (74%),** and their national identity number and/or card number or passport number (73%). Thus, alongside financial and identity data, medical information is considered very personal by a large majority of Europeans.

A second group of data, which appears to be closely tagged to the individual, and is considered personal by most Europeans, includes fingerprints (64%), home address (57%), mobile phone number (53%), photos of people (48%), and their name (46%). A third group, identified as social information follows: about a third of EU people, consider as personal their work history (30%) and who their friends are (30%); around a quarter of respondents also think that information about their tastes and opinions (27%), their nationality (26%), things they do, such as hobbies, sports, places they go (25%), and the websites they visit (25%) is personal.

To confirm the complementarities of types of personal data,[68] factor analysis was used to categorise items into various themes or factors.[69] This analysis yields three statistically significant and conceptually meaningful factors [Table 78]. the first factor groups information related with social activities as activities; preferences; friends; websites visited; work history and photos. In other words, people who consider one item as personal are also very likely to consider the next item in the factor as personal. The first factor includes mostly 'social' information, and was therefore labelled "social information". The second factor includes name, address, nationality and mobile number. This information may be interpreted as "identifiers" – that is items of information generally used to identify people in identity management systems, online and offline. Finally, the third factor includes financial information, medical information and fingerprints. Thus, this factor is labelled as "sensitive information", as most people consider it personal, as it was discussed above.

To sum up, there are three main types of information people considered personal 'jointly': social information, identifiers and sensitive information. Not surprisingly, medical information is grouped as sensitive information. We then looked in greater depth at medical information as personal information, to see whether there are differences based on socio-demographic traits of respondents and across EU27 countries.

From a socio-demographic point of view [Table 79], females (75%) are slightly more likely than males (72%) to consider medical information as personal. Age also appears to play a role: middle age interviewees, especially those between 25-39 (75%) and 40-54 (76%), are slightly more likely to consider medical information to be personal than younger (71%) or

68 We have excluded from the factor analysis "Your national identity number \ card number\ passport number" due to the different documents, if any, used in EU27 and the different regulations regarding the allocation and use of national identity numbers.

69 An analysis of the correlation matrix (KMO and Bartlett's test of sphericity) was carried out to check that the correlation matrixes were factorable. Data reductions were undertaken by principal components analysis using the Varimax option to identify possible underlying dimensions.

Table 77. Information and data considered as personal

Financial information (e. g salary, bank details, credit record)	75%
Medical information (patient record, health information)	74%
Your national identity number \ card number\ passport number	73%
Your fingerprints	64%
Your home address	57%
Your mobile phone number	53%
Photos of you	48%
Your name	46%
Your work history	30%
Who your friends are	30%
Your tastes and opinions	27%
Your nationality	26%
Things you do (e.g. hobbies, sports, places you go)	25%
Websites you visit	25%
None (SPONTANEOUS)	1%
DK	1%

Base: EU27.

Source: QB2.

Table 78. Factor analysis of data and information considered as personal

	Factor 1. Social information	Factor 2. Identifiers	Factor 3. Sensitive information
Your tastes and opinions	.82		
Things you do (e.g. hobbies, sports, places you go)	.81		
Who your friends are	.78		
Websites you visit	.69		
Your work history	.64		
Photos	.50		
Your name		.85	
Your home address		.84	
Your nationality	.50	.57	
Mobile number		.47	.46
Medical information (patient record, health information)			.76
Financial information (e. g salary, bank details, credit record)			.76
Your fingerprints			.58
Auto values	5.13	1.51	1.15
% Variance explained	39.5	11.6	8.9

Base: EU27.

Source: QB2.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0.896; Bartlett's test of sphericity p=0.000; Convergence in 5 iterations; Minimum eigenvalue 1; Values below .04 are omitted.

Table 79. Medical information considered as personal information by socio-demographic traits

		No	Yes
Gender	Male	28%	72%
	Female	25%	75%
Age [brackets]	15-24	29%	71%
	25-39	25%	75%
	40-54	24%	76%
	55+	28%	72%
Terminal education age	15-	33%	67%
	16-19		
	20+	19%	81%
	Still Studying	29%	71%
Occupation	Self-employed		
	Managers	17%	83%
	Other white collars	22%	78%
	Manual workers		
	House person	32%	68%
	Unemployed	31%	69%
	Retired	29%	71%
	Students	29%	71%
Difficulties to pay bills	Most of the time	31%	69%
	From time to time	30%	70%
	Almost never/ never	24%	76%
Personal mobile phone	No	37%	63%
	Yes	25%	75%
Internet use	No	35%	65%
	Yes	22%	78%

Base: EU27.

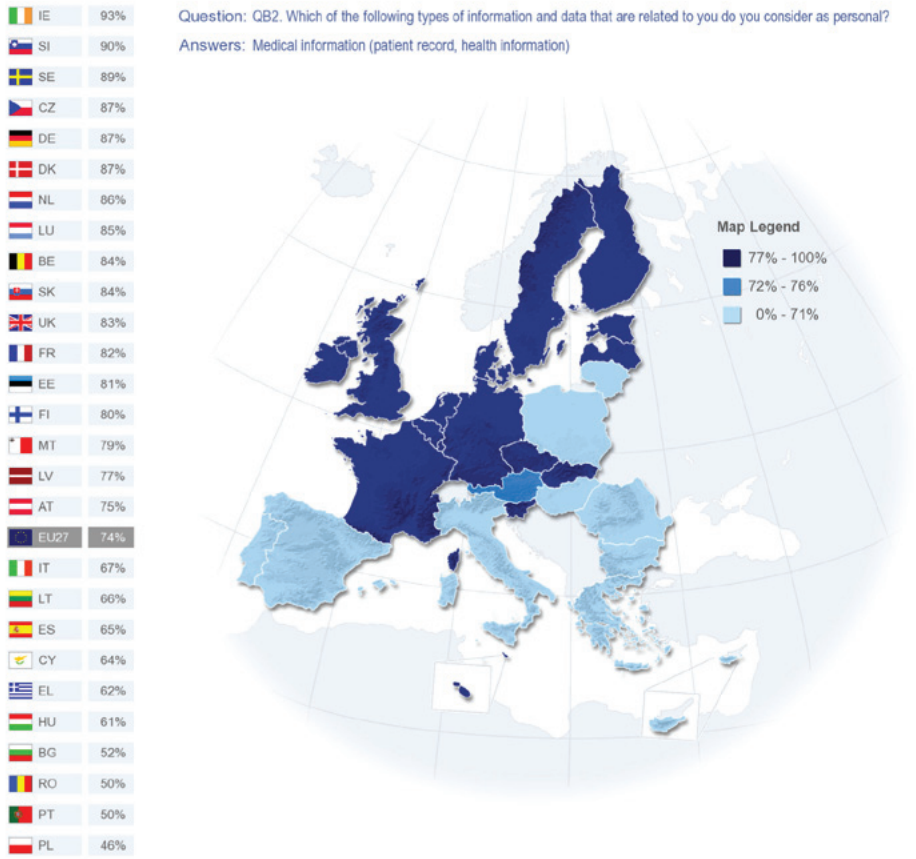
Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

elderly (72%) interviewees. Younger individuals (15-24) are more likely to be healthy and may not worry as much about their health, however 71% of them considered medical information as personal vs. 29% who did not consider this type of information as personal. It could be argued that even if younger individuals should not worry about their health status, they are significantly concerned about the medical information, and therefore they consider it as personal information. Elderly individuals (55+), who are more likely to be worried about their health and have a higher probability to suffer a health problem, are less likely to consider medical information as personal but not by much.

Several differences also appear in terms of education and occupation. Interviewees with lower levels of formal education (terminal education age lower than 16) or still studying are less likely to consider medical information to be personal (67% and 71% respectively), than those with higher levels of formal education (20+) (81%). On the contrary, managers (83%) and other white collar workers (78%) are more likely to consider medical information more personal than house people (68%), unemployed (69%), retired (71%) or students (71%). Furthermore, interviewees who have difficulties to pay bills most of the time (69%) are less likely to consider medical information to be personal, than those who have these difficulties from time to time (70%) and almost never or never (76%). Finally, individuals who have a personal mobile phone (75%) and use the Internet (78%) are more likely to consider medical information to be personal than those who do not have a personal mobile phone (63%) and do not use the Internet (65%).

These characteristics reveal a small socio-economic divide in the perception of the importance of personal medical data between

Figure 28. Medical information considered personal data by country



Base: EU27.

well educated, white collar, wealthy respondents, and those with lower education, outside the labour market and less wealthy. These results may be natural, and people in the former category have more health choice than people solely relying on national health systems, where lesser choice may be available. However, it also points to a significant disparity in the perception of one's own health, as people from poorer backgrounds may be less protective of their medical data privacy than wealthier Europeans.

At country level, a large majority of European interviewees see medical information as personal. But respondents located in the north and west of the European Union are most likely to regard medical information as personal [Figure 28]. Medical information comes forward as personal before other types of information, namely financial and identity information, in the following Member States: Ireland (93%), Slovenia (90%), Sweden (89%), Belgium (84%), and France (82%). Large majorities of respondents who believe that medical information is personal are also found in the Czech Republic, Germany, Denmark (each 87%), the Netherlands (86%), Slovakia (84%), the United Kingdom (83%), Estonia (81%) and Finland (80%). Countries where only around half of the respondents think so are Poland (46%), Portugal and Romania (each 50%) and Bulgaria (52%). In these Member States, identity credentials, such as identity cards and passports, are deemed to be personal by a vast majority of people (84%, 73%, 81%, 92% respectively). If the latter indicates that where traditional identifiers dominate, sensitive information is seen as 'less sensitive', it nevertheless does not appear to reflect

influence from institutional or health care system characteristics nor welfare state models.[70]

5.4 Management of personal data by other parties, trust, concern and value

We then asked a range of questions concerning the management of personal information by other parties, on behalf of the individual. Different authorities (government departments, local authorities, agencies) and private companies routinely collect and store personal data. Questions were asked on approval, on trust in data handlers and on concern about use of personal data.

First, individuals were asked if specific approval should be required before any kind of personal information is collected and processed. A large majority say their approval should be required in all cases (74%). Only around one in ten says so in the case of personal information collected on the Internet (12%), or in the case of sensitive information (health, religion, political beliefs or sexual preferences - 8%). Individuals who stated that specific approval should be required are more likely to consider medical information as personal (55%) than those who do not consider medical information as personal information (45%). Furthermore, individuals who stated that specific approval should be required in all cases are more likely to consider medical information as personal (76%) than individuals who do not consider this type of information as personal (24%).

Second, respondents were asked to what extent they trust institutions to protect their personal information [Table 80]. Individuals who considered medical information as personal are more likely to trust health and medical institutions (86%), national public authorities (73%), and banks and financial institutions (66%) than those who did not consider medical information as personal (74%, 68%, and 59% respectively). On the contrary, they are less likely to trust shops and department stores (62%); internet companies (73%), and phone companies (68%) than those who do not consider medical information as personal information (44%, 49% and 62% respectively).

These results point out the difficulties that shops, Internet, phone and mobile companies and ISPs may have to launch and/or maintain any health business initiative which implies the disclosure of medical information, due to the importance of trust in the health field.[71] On the other hand, national public authorities, banks and financial institutions and specially health and medical institutions could benefit from this level of trust to launch or support this kind of initiatives (as Personal Health Records).[72] Furthermore, banking on health has been pointed out as a possible way to allow individuals to access upload and control their medical information.[73] This could be framed in Digital Agenda for Europe (Pillar ICT for Social Challenges) under Action 75: Give Europeans secure online access to their medical health data and achieve widespread telemedicine deployment.

70 Klazinga N, Fischer C, Ten Asbroek A. (2011) Health services research related to performance indicators and benchmarking in Europe. Journal of Health Services Research & Policy;. 16(2):38-47.
Simonazzi A. (2009). Care regimes and national employment models- Cambridge Journal of Economics; 33: 211-232.

71 Recently Google has announced that its Personal Health Record Google Health will be retired on 1 January 2012 http://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html

72 Archer N, Fevrier-Thomas U, Lokker C, McKibbon KA, Straus SE (2011) Personal health records: a scoping review J Am Med Inform Assoc.18(4):515-22.

73 Ball MJ, Gold J. (2006). Banking on health: Personal records and information exchange. J Health Inf Manag. 20(2):71-83 and Ball MJ, Costin MY, Lehmann C. (2008). The personal health record: consumers banking on their health. Stud Health Technol Inform.134:35-46.

Table 80. Trust in data controllers and medical information considered as personal data

		Medical information as personal	
		No	Yes
National public authorities	Do not trust at all	10%	8%
	Tend not to trust	22%	19%
	Tend to trust	52%	53%
	Totally trust	16%	20%
European institutions*	Do not trust at all	12%*	12%*
	Tend not to trust	28%*	26%*
	Tend to trust	48%*	49%*
	Totally trust	12%*	12%*
Banks and financial institutions	Do not trust at all	12%	11%
	Tend not to trust	29%	23%
	Tend to trust	46%	49%
	Totally trust	13%	17%
Health and medical institutions	Do not trust at all	8%	5%
	Tend not to trust	18%	14%
	Tend to trust	54%	55%
	Totally trust	20%	26%
Shops and department stores	Do not trust at all	16%	21%
	Tend not to trust	38%	41%
	Tend to trust	40%	34%
	Totally trust	6%	4%
Internet companies	Do not trust at all	29%	33%
	Tend not to trust	40%	43%
	Tend to trust	27%	22%
	Totally trust	4%	2%
Phone companies, mobile phone companies and Internet Services Providers	Do not trust at all	23%	28%
	Tend not to trust	39%	40%
	Tend to trust	33%	29%
	Totally trust	5%	3%

Base: EU27.

Source: QB25.

*Note: * No significant difference was found.*

Companies holding personal information may sometimes use it for a purpose other than that for which it was collected (e.g. for direct marketing or targeted online advertising), without informing the individuals concerned. Respondents were asked how worried they were about this use of their information [Table 81]. Individuals who considered medical information as personal are slightly more likely to be concerned (74%) than those who did not consider this type of information as personal (66%).

We then checked the relationship between trust and concern [Table 82], in relation to personal health information. Overall, individuals who consider medical information as personal are more likely to be concerned about stealth re-use of their personal data than individuals who did not consider it personal, regardless of whether they trust or not data controllers. On the one hand, individuals who consider medical information as personal and trust national public authorities, banks and financial institutions and health and medical institutions are more likely

Table 81. Concern about unannounced re-use of personal data for different purpose than original and medical information considered as personal data

	Medical information as personal	
	No	**Yes**
Not at all concerned	8%	5%
Not very concerned	26%	21%
Fairly concerned	46%	46%
Very concerned	20%	28%

Base: All individuals.
Source: QB26.

Table 82. Concern about unannounced re-use of personal data by trust in data controllers and medical information considered as personal data

		Medical information as personal	
		No	**Yes**
		% concerned	**% concerned**
National public authorities	Not trust	68%	82%
	Trust	66%	71%
Banks and financial institutions	Not trust	69%	81%
	Trust	65%	71%
Health and medical institutions	Not trust	67%	81%
	Trust	66%	73%
European institutions	Not trust	70%	82%
	Trust	64%	70%
Shops and department stores	Not trust	73%	80%
	Trust	59%	66%
Internet companies (Search Engines, SNS, E-mail Services)	Not trust	72%	80%
	Trust	58%	60%
Phone and mobile phone companies and Internet Services Providers	Not trust	73%	79%
	Trust	58%	64%

Base: All individuals.
Source: QB25.

to be concerned (approximately 70%) than individuals who did not consider this type of information as personal (approximately 65%). That is, trust makes very little difference to people who do not consider medical information as personal, but a large difference for those who consider their medical data to be personal. On the other hand, trust is extremely important, almost critical, for shops and department stores, Internet companies, phone and mobile phone companies. In this case, trust matters a lot for all, in that trust is associated with significantly lower values of percentage of concerned across the sample, for both people who consider medical data as personal and otherwise.

Finally, people were asked about their willingness to pay for access to personal data

Table 83. Willingness to pay for access to personal data

		Yes, but only a small amount (e.g. postage or communication costs)	Yes, up to 20 Euro	Yes, more than 20 Euro	No	DK
Medical information considered as personal information	No	15%	6%	3%	66%	9%
	Yes	21%	8%	2%	65%	4%

Base: EU27.

Source: QB27.

Note: Only significant difference at $p < 0.01$ are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

held by data controllers [Table 83].[74] Respondents who considered medical information as personal are slightly more likely to be willing to pay for access to personal data in the case of only small amount of money (21%) and up to 20 euros (8%) than those who did not consider this type of information as personal (15% and 6% respectively). Nevertheless, two-thirds of respondents (about 66%) are not prepared to pay at all.[75]

5.5 Awareness and protection of personal data

We found that considering one's medical data as personal is associated with increased levels of awareness and a higher desire for strong protection of one's personal data.

Respondents were asked whether they heard of or experienced issues related to data loss and identity theft in the last 12 months.[76] Respondents who considered medical information as personal are more likely to have heard about it through television, radio, newspapers, the Internet (45% media awareness) than those who did not consider it as personal (32%). Social awareness (word of mouth and/or acquaintance) and self-family experience (you directly and/or a member of your family) were not found to be statistically significant. This emphasises the importance of media in health communication campaigns to raise awareness as to risks related to data loss or theft. Moreover, respondents who consider medical information as personal are more likely to have heard about a public authority in their countries responsible for protecting their rights regarding personal data[77] (36%) than those who did not consider this type of information as personal (28%).

Furthermore, respondents who considered medical information as personal are more likely to state that they would want to be informed by a public authority or by a private company whenever information they hold about them is lost or stolen[78] (91% vs. 78%) and to have the same rights and protections over their personal information regardless of the EU country in which it is collected and processed[79] (79% vs. 57%). Also, those who consider medical information as personal are more likely to state that the enforcement of the rules on personal

74 QB27. According to EU data protection rules, you have the right to access your personal information stored by public or private entities, in order to change, block or delete it. EU rules do not specify whether access to personal information should be free of charge. In some EU Member States, you have to pay in order to be granted such access. Would you be prepared to pay to have access?

75 Financial information follows the same pattern as medical information

76 QB30. In the last 12 months, have you heard about or experienced issues in relation to data losses and identity theft?

77 QB38. Have you heard about a public authority in (OUR COUNTRY) responsible for protecting your rights regarding your personal data?

78 QB31. Would you want to be informed by a public authority or by a private company whenever information they hold about you is lost or stolen?

79 QB32. How important or not is it for you to have the same rights and protections over your personal information regardless of the EU country in which it is collected and processed?

data protection should be dealt with at European level[80] (47%) than those who did not consider it as personal (38%).

5.6 Medical information and social computing

5.6.1 User characteristics of Social Networking Sites and their use of medical information

Social Computing is defined as "a set of open, web-based and user-friendly applications that enable users to network, share data, collaborate and co-produce content" and has become "an important social phenomenon, in terms of reach, time-use and activities carried out".[81] In the health arena, the concept of Health 2.0[82] has emerged to examine the role of social computing within health, seen as creating several opportunities and challenges in relation with the disclosure of medical information. On the one hand, the participation, collaboration and interaction of social computing users[83] around health issues within SNS and/or websites to share pictures, videos, experiences and intelligence could facilitate their empowerment and have a positive impact on their health. On the other hand, the context and quality of information shared, the health literacy of the individuals accessing it, privacy, confidentiality, control of information, could inhibit the positive impact or even have a negative impact on their health.

The current prevalence of social computing is reflected in the number of users. Slightly over half of all internet users (52%) use a social networking site and more than four in ten (44%) use websites to share pictures, videos, movies, etc. Socio-demographic characteristics that influence social networking and sharing sites are age, education, occupation, financial situation, household composition and frequency of Internet use. Specifically, younger age cohorts (15-24 and 25-39) are more likely than the older age cohorts (40-55 and 55+) to undertake both activities. Also, Internet users with higher education, those who studied until the age 20 or later, are more likely to engage in these activities than users who left school at the age of fifteen or younger: using social networking sites (48% vs. 35%), and using sharing sites (40% vs. 30%). Then, interviewees who use the Internet every day undertake both activities more often than average: social networking sites (60%), and sharing sites for pictures and the like (51%).

In terms of geography, high rates of social networking use are found in smaller in population and newer in joining the European Union Member States. Social networking sites are used most often by internet users in Hungary (80%), Latvia (73%), Malta (71%), Ireland (68%), Cyprus, Slovakia (both 66%), Poland and Denmark (both 63%), and least in Germany (37%), Italy, Czech Republic (both at 48%), Austria (49%) and France (50%). Websites for sharing files are particularly popular in eastern and southern Member States. A majority of Internet users in mostly eastern and southern EU Member States use websites to share pictures, videos and movies: Bulgaria, Lithuania (both 59%), Cyprus, Slovakia and Ireland (all 58%), Romania, Latvia (both 56%), Greece, Hungary and Spain (all 53%), as compared to around one-third of those in Germany (32%), Finland (35%) and France (39%).

The respondents who use SNS and sharing sites (to identify this group of users, we name them social computing users) were then asked which types of personal information they

80 QB37. In your opinion, the enforcement of the rules on personal data protection should be dealt with at…?

81 Punie, Y., Lusoli, W., Centeno, C., Misuraca, G., & Broster, D. (2009) (Eds.). The impact of Social Computing on the EU Information Society and Economy (JRC Scientific and Technical Reports No. EUR 24063 EN). Brussels: JRC

82 Van De Belt TH, Engelen LJ, Berben SAA, Schoonhoven L Definition of Health 2.0 and Medicine 2.0: A Systematic Review J Med Internet Res 2010;12(2):e18.

83 Users could be patients, medical professionals, formal and informal carers and supportive relatives.

disclosed in these environments.[84] We found that only 5% disclose medical information on SC sites. By means of comparison, we also found that only 3% of Internet users disclosed medical information in the context of eCommerce.

Indeed, people mostly share **social information** on SC sites but also basic identity information: almost eight out of ten social computing users, revealed their name (79%) and around half disclosed photos of themselves (51%) or their nationality (47%). Almost four in ten disclosed the things they do (for example hobbies, sports, places they go), their home address, and who their friends are (all three 39%). One-third shared their tastes and opinions (33%) and a quarter gave their mobile phone number (23%). Fewer respondents disclosed their work history (18%), their national identity number, identity card number, or passport number (13%). Financial information such as salary, bank details and credit record (10%), and medical information such as patient record and health information (5%) are unlikely to be disclosed on SC sites.

Factor analysis was carried out to check the complementarities of the personal information disclosed in SNS and sharing sites.[85] This analysis [Table 84] identified three conceptually meaningful factors. The first factor includes who friends are; photos; activities; preferences and websites visited. Therefore, it is labelled "social information". The second factor groups fingerprints, medical information and financial information. These types of information disclosed are related with "sensitive information". Finally, the third factor tackles national identity number; address; mobile number; name and nationality. Thus, this factor is labelled as "traditional identifiers". This may be a slight misnomer, as 'mobile phone' is included in the group. However, all other items are personal information used as identifiers in many government and commercial transactions. To sum up, there are three main types of information Social Computing users disclose 'jointly': Social information; Sensitive information and Traditional identifiers.

We then took jointly into account Social Computing users' behaviours (what data they actually disclose) and perceptions (what they thought are personal data.) This allowed us to profile four different types of individuals [Table 85]. The first two groups include 'self-revealing' social computing users who disclose medical information (5%). Within this group we can identify those who consider this type of information as personal (4%) and those who do not consider it as personal (1%). Even though both groups are generating online medical information contents, different perceptions of this type of information as personal raises a different level of awareness and caution. But a majority of social computing users do not disclose medical information (95%). Within this group are individuals who consider medical information as personal (73%) and this group may be labelled as "Cautious" and individuals who do not consider it as personal (22%) and the second group may be labelled as "Indifferent".

Due to the small number of social computing users who disclose medical information, we examine here three groups only: social computing users who disclosure medical information (**self-revealing - 5%**); social computing users who do not disclosure medical information and consider it as personal (**cautious - 73%**) and social computing users who do not disclosure medical information and do not consider this type of information as personal (**indifferent - 22%**).

We started by looking at the socio-demographic differences, if any, among these groups [Table 86]. To put results in perspective, it should be kept in mind that we are talking of

84 QB4a Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?

85 An analysis of the correlation matrix (KMO and Bartlett's test of sphericity) was carried out to check that the correlation matrixes were factorable. Data reductions were undertaken by principal components analysis using the Varimax option to identify possible underlying dimensions.

Table 84. Factor analysis of personal information disclosed in social computing

	Factor 1. Social information	Factor 2. Sensitive information	Factor 3. Traditional identifiers
Who friends are	.76		
Photos	.75		
Activities	.75		
Preferences	.73		
Websites visited	.46		
Work history			
Fingerprints		.76	
Medical information		.75	
Financial information		.69	
National Identity number		.61	.33
Address			.81
Mobile number			.67
Name	.31	-.35	.58
Nationality	.42		.51
Auto values	3.108	2.428	1.556
% Variance explained	22.199	17.346	11.111

Base: SC users.

Source: QB4a. Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?.

Notes: Rotated components matrix; Sampling method: factor analysis by main components; Rotation method: Varimax with Kaiser-Meyer-Olkin 0. 786; Bartlett's test of sphericity p=0.000; Convergence in 4 iterations; Minimum eigenvalue 1; Values below .03 are omitted.

Table 85. Social computing users and medical information

		Medical information disclosure	
		Yes	No
Medical information as personal	Yes	4%	73%
	No	1%	22%

Base: SC users.

Source: QB2.1 & QB4a1.

internet users who also use social computing sites. **Self- revealing** users are more likely to be in the older age (40-54 and 55+ cohorts (25% and 14% respectively); to end education at the age of 16-19 (46%); to live in a house with three persons (28%); not to have difficulties to pay their bills; and to be heavy Internet users at home. **Cautious** users are slightly more likely to be female; to be 15-24 (29%) or 55+ (12%); to be students (19%) or manual workers (23%); to end education at the age of 16-19 (41%) or 20+ (34%); to live in a house with 4+ (34%); not to have difficulties to pay their bills; and to be heavy Internet users at home and at work. **Indifferent** users are slightly more likely to be male (56%); to be 15-24 (38%); to be student (26%); to be still studying (25%) or end education at 20+; not to have difficulties to pay their bills; and to be heavy Internet users at home and at work. Finally, **self-revealing** Internet users are more likely to be using the Internet in more sophisticated ways (r. = .33 correlation with advanced software activities); **cautious** users carry out more eCommerce and eGovernment transactions (r = .20) – which may be the reason they are indeed cautious; while **indifferent** SC users are less likely to do either (that is, they largely carry out ordinary Internet activities, email and search).

More specific differences include:

- Cautious users are more likely to be female while indifferent individuals are more likely to be male. This characteristic

Table 86. Characterisation of social computing users and medical information perception and behaviours

		Medical information		
		Disclosed (self-revealing)	Not Disclosed	
			Personal (cautious)	Not Personal (indifferent)
Gender	Male		49%	56%
	Female		51%	44%
Age	15-24	30%	29%	38%
	25-39			
	40-54	25%		
	55+	14%	12%	6%
Occupation	Self-employed		8%	9%
	Managers	9%	14%	11%
	Other white collars			
	Manual workers		23%	
	House person			5%
	Unemployed		9%	
	Retired		8%	4%
	Students		19%	26%
Terminal education age	15-			
	16-19	46%	41%	
	20+		34%	25%
	Still Studying		19%	25%
Household composition	1		16%	12%
	2		18%	5%
	3	28%		
	4+		34%	42%
Difficulties to pay your bills	Most of the time	15%		
	From time to time	40%	29%	36%
	Almost never/ never	45%	61%	55%
Internet use at home	Every day/Almost every day	67%	81%	74%
	Two or three times a week	23%	12%	15%
	About once a week		3%	5%
Internet use at work	Every day/Almost every day		35%	25%
	Two or three times a week	9%	5%	7%
	About once a week	3%		
	Two or three times a month		61%	33%

Base: Social computing users.

Source: QB2.1 & QB4a1.

*Note: Only significant difference at $p < 0.01$ are reported [i.e. when there is a 99% probability that the relation reported is not due to chance] * Adjusted residual >1.9.*

points out the importance of women regarding health issues.

- If we consider that individuals above 40 have more probability of having a health problem (especially those above 55+) or being responsible of caring for their families, it is not surprising that self-revealing individuals are more likely to be older than cautious and indifferent individuals (this profile is the youngest one).

- Due to the age characterization cautious and indifferent individuals are more educated than self-revealing individuals. Nevertheless, the education level of self-revealing individuals remains high so the risk of health illiteracy could be decreased and the positive impact of disclosing medical information on their health outcomes or the health outcomes of their family would be higher. Furthermore, the role of health information to empower

Table 87. National differences of social computing users and medical information perception and behaviours

	% of Internet users who used Internet for health purposes*	Medical information**		
		Disclosed (self-revealing)	Not Disclosed	
			Personal (cautious)	Not Personal (indifferent)
France	46	1	82	17
Luxemburg	65	1	87	12
Sweden	45	3	88	9
United Kingdom	39	3	84	13
Germany	60	3	83	14
Denmark	59	3	89	8
Bulgaria	31	3	54	42
Cyprus	41	3	61	35
Finland	67	3	81	16
Poland	43	4	49	48
The Netherlands	56	4	83	12
Latvia	49	4	76	20
Greece	50	4	60	36
Lithuania	51	5	72	24
Slovenia	64	5	87	8
EU27	50	5	73	22
Malta	54	6	74	21
Slovakia	64	6	79	15
Belgium	47	7	81	12
Portugal	59	7	57	36
Czech Republic	31	8	82	11
Hungary	65	8	58	34
Italy	45	8	60	32
Ireland	41	9	82	9
Spain	53	9	61	30
Romania	53	12	48	40
Austria	50	12	65	23
Estonia	47	13	72	16

Base:

** % of Internet users who used Internet for health purposes. EUROSTAT 2010 ICT Household survey.*

***SC users.*

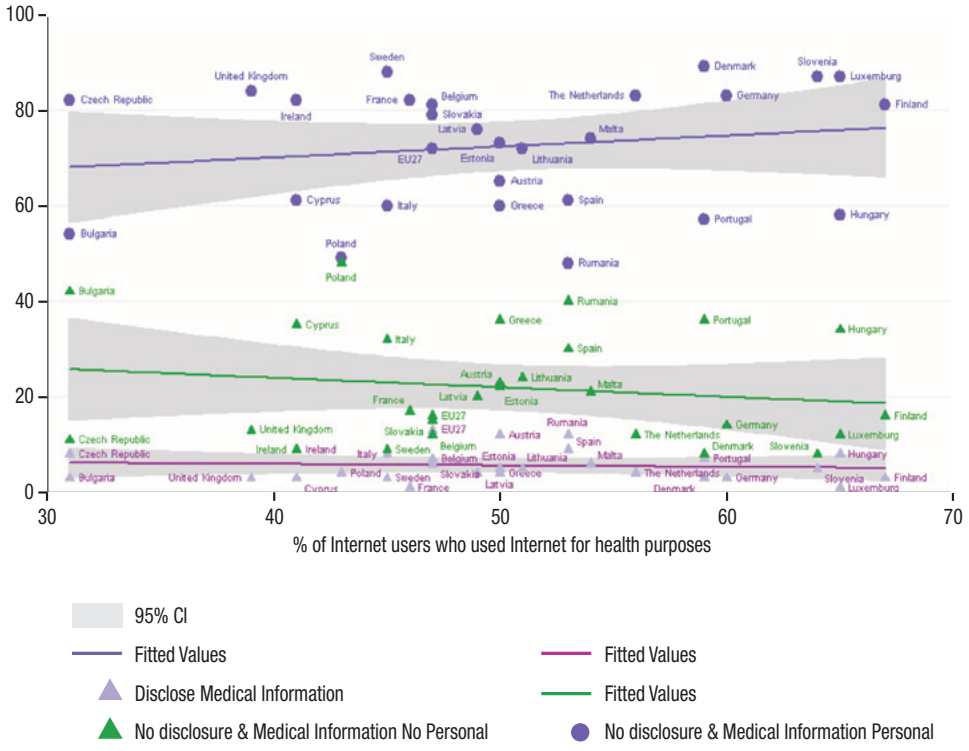
individuals could be increased with a positive impact on health outcomes.

- The fact that household composition is statistically significant reveals the importance of social life of medical information and emphasises the role of the individuals as mediators of health information.

It is worth pointing out that predictors of Internet use and social computing use (young age, wealth, household composition, education) are also related with social determinants of health. Thus, while self-revealing individuals have a slightly lower socio-economic status than cautious and indifferent individuals (education and difficulties to pay bills), they are in a better socio-economic status than people who do not use the Internet (67% self-revealing individuals use the Internet at home every day or almost every day and 23% use it two or three times a week).

Regarding national differences [Table 87], the highest percentage of social computing respondents who disclose medical information (**self-revealing**) are to be found in Estonia (13%), Austria (12%) and Romania (12%). In contrast, respondents in France (1%) and Luxemburg (1%)

Figure 29. Social computing users and Internet users who use the Internet for health purposes at country level



Base: EU27.

are least likely to disclose medical information. The **most 'indifferent'** respondents tend to be in Poland (48%), Bulgaria (42%) and Romania (40%) while the least 'indifferent' respondents are to be found in Slovenia and Denmark (each with 8%) and in Sweden and Ireland (each with 9%). Finally, the **most 'cautious'** respondents are to be found in Denmark (89%), Sweden (88%) and Luxemburg (87%) while the least 'cautious' respondents are to be found in Romania (48%), Poland (49%) and Bulgaria (54%). While there is a marked absence of pattern that could give rise to a logical interpretation of the reasons why this is happening, the case of Austria[86] with a relatively high number of self-revealing users (12%), with a relatively low number of 'cautious' users (65%) and a relatively high number of 'indifferent' users (23%) seems to define a future trend to further explore. This indicates that there are benefits to sharing health-related information on SC sites (see Table 88 for an analysis of the reason to disclose), and when managed appropriately it lowers concerns and empowers the users.

Looking at the wider picture, we examine whether there is a relation between Internet use for medical information in a country,[87] and disclosure of medical information in the context of social networking (self-revealing, cautious, indifferent). In short, the correlation is weak for all three behaviours across EU27 [Figure 29]. The absence of patterns indicates the lack of network effect in the number of users generating medical information content and the number of users seeking health information on the Internet. Medical information on the Internet at large and

86 AT is a Member State with relatively high Internet use, where electronic Identity management exists, including in the health area, is functional and relatively diffused, the citizens of which are well aware of Data protection regulation.

87 Source: EUROSTAT 2010 ICT HOUSEHOLD SURVEY % of Internet users who used Internet for health purposes.

disclosure of online personal data appear to be unrelated at country level.

5.7 Reasons to disclose medical information in SNS

We examined the relation between disclosure of medical information in social computing and the general reasons why people disclose information on such sites [Table 88]. The two main reasons given by respondents for the disclosure are to access the service (61%) and to connect with others (52%). Around one-fifth of the respondents do so for fun (22%), to obtain a service adapted to their needs (18%), or to get a service for free (18%). People who self-reveal medical information appear to disclose (in general), for pragmatic reasons: they are more likely to disclose to get a service for free; to save time at the next visit; to benefit from personalised commercial offers and to receive money or price reduction. On the contrary, they are less likely to disclose information to connect with others or for fun.[88]

This trend could support a niche market of digital health services as health personal records or SNS to support groups of individuals with the same health problems, especially chronic conditions. However we have to emphasise the importance of trust in relation with health (see Table 82 with data on what institutions are more trusted). On the other hand, we also need to take into account that the group of indifferent users is sharing health related information that they think can hardly be

Table 88. Reasons to disclose personal data in social computing and medical information disclosed in social computing sites

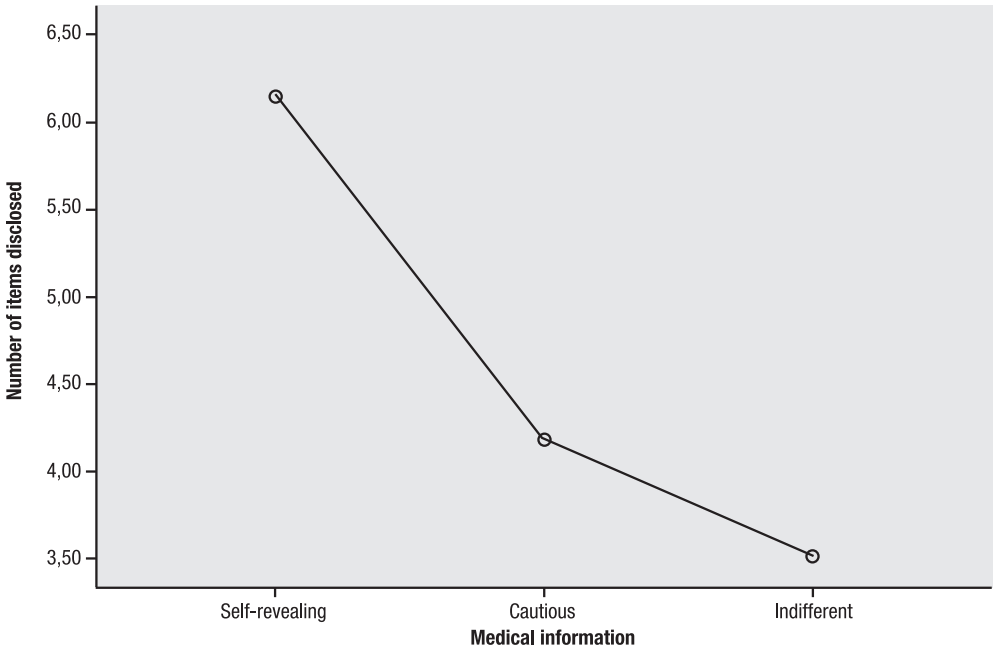
		Total Social Computing users	Medical information		
			Disclosed (self-revealing)	Not disclosed	
				Personal (cautious)	Not Personal (indifferent)
To access the service	Yes	61%			
To connect with others	Yes	52%	27%	56%	43%
For fun	Yes	22%	12%	23%	21%*
To obtain a service adapted to your needs	Yes	18%			
To get a service for free	Yes	18%	26%	17%	19%
To save time at the next visit	Yes	12%	25%		
To benefit from personalised commercial offers	Yes	8%	15%	7%	8%*
To receive money or price reduction	Yes	6%	18%	5%	7%*

Base: SC users.

*Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance] * Adjusted residual >1.9.*

88 Financial information follows the same trend as medical information does.

Figure 30. Number of items disclosed and medical information disclosed



Note: ANOVA p<.000.

considered a risk or raise concern (i.e. disease-related information that is clearly curable and has no future consequences for the individual such as: fever, appendix problems, chickenpox, etc…).

It is also interesting to note that whether it is considered as personal or not, the information disclosed [e.g. cautious and indifferent types] makes little difference in terms of the reasons why people disclose. The only statistically important difference relates to the reason "connecting with others", which is more significant as a reason for 'cautious' users than for 'indifferent' users. Again, this underlines the importance of the nature of the information actually disclosed, rather than of the perceptions: people who are cautious in relation to their medical information (therefore aware) need not be cautious in relation to data of social nature disclosed [Figure 30]. In essence this means that while self-revealing individuals are behaving consistently for all types of data (including health-related information), cautious individuals who are concerned about revealing their health information are instead more likely to disclose other items on Social Computing sites than indifferent individuals, who share very few data overall.

5.8 Risks, informed consent and responsibility

Social Computing users were asked which three (out of ten) potential risks they associated with disclosure of personal information.[89] Around four in ten respondents mention information being used without their knowledge (44%), being victim of fraud (41%) and information being shared with third parties without their knowledge (38%). Around one-third mention the risk of identity theft online (32%) and that the information will be used to enable sending them unwanted commercial offers (28%). About a quarter of respondents fear that the information will be used in different contexts from the ones where they disclosed it (25%). Just 3% of respondents stated spontaneously that they perceive no risks. Self-revealing SC users are more likely to perceive reputation damage and misunderstanding of their views and behaviors connected with disclosure of personal information [Table 89].

89 QB7a I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information on social networking sites and\ or sharing sites?

Table 89. Risk perception and medical information disclosed in SC sites

	Total SC users	Medical information		
		Disclosed (self-revealing)	Not disclosed	
			Personal (cautious)	Not Personal (indifferent)
Your information being used without your knowledge	44%	36%	46%	40%
Yourself being victim of fraud	41%			
Your information being shared with third parties without knowledge	38%	31%	41%	30%
Your identity being at risk of theft online	32%	31%	34%	29%
Your information being used to send you unwanted commercial offers	28%	18%		25%
Your information being used in different contexts	25%	20%	27%	19%
Your personal safety being at risk	20%			
Your reputation being damaged	12%	19%		
Your views and behaviours being misunderstood	11%	17%		
Yourself being discriminated against	7%			5%
None (SPONTANEOUS)	3%		2%	4%

Base: SC users.

Source: QB7a.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

SC users were then asked whether service providers sufficiently inform their users about the possible consequences of disclosing personal information.[90] Almost half of the respondents say they are sufficiently informed (52%). However, an almost equal proportion says that they are not (48%). This point is very important, as it is at the core of the informed consent principle of data protection regulation in Europe. Although informed consent relates largely to the uses that will be made of the data, and not to the possible consequences, the latter are most important for users. SC users who disclosed medical information (self-revealing) are more likely to consider that these sites sufficiently inform their users about the possible consequences of disclosing personal information (65%) than SC users who did not disclose this type of information (47% cautious and 61% indifferent) [Table 90]. Once again, considering one's data as personal may be more accurate than actual disclosure to explain people's perceptions of data protection in the SC environment.

Concerning responsibility, SC users were asked who should take care of the information they have disclosed.[91] Firstly, half of the respondents point to themselves (50%), while one-third point to the social networking or sharing sites (33%). Even fewer respondents mention public authorities (17%). When the interviewees are given the opportunity to name a second responsible entity or person

90 QB8a. Please tell me whether you agree or disagree with the following statement: social networking sites and/ or sharing sites sufficiently inform their users about the possible consequences of disclosing personal information.

91 QB9a Who do you think should make sure that your information is collected, stored and exchanged safely on social networking sites and/ or sharing sites? Firstly? And secondly?

Table 90. SNS sufficiently inform their users about the possible consequences of disclosing information by disclosure of medical information

	Total SC users	Medical information		
		Disclosed (self-revealing)	Not disclosed	
			Personal (cautious)	Not Personal (indifferent)
Totally disagree	18%	13%	21%	11%
Tend to disagree	30%	22%	32%	28%
Tend to agree	39%	47%	35%	48%
Totally agree	13%	18%	12%	13%

Base: SC users.

Source: QB8a.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

(secondly), the total results mention social networking or sharing sites (43%), the public authorities (30%) and themselves (27%). While we found no specific patterns here, self-revealing respondents are slightly more likely to give overall responsibility to public authorities firstly (20%) than respondents who do not disclose medical information (17%). Overall, therefore, attribution of responsibility appears stable regardless of disclosure and perception of medical information.

5.8.1 Attitudes towards the disclosure environment: trust, approval and concern regarding re-use of personal data

National public authorities and European institutions are considered as the most trusted institutions by SC users who disclose medical information (self-revealing). These individuals are more likely to trust national public authorities (80%) than cautious (76%) and indifferent (71%) [Table 91]. Furthermore, even though the level

Table 91. Trust in data controllers and medical information disclosed

		Medical information		
		Disclosed (self-revealing)	Not disclosed	
			Personal (cautious)	Not Personal (indifferent)
National public authorities	Do not Trust	20%	24%	29%
	Trust	80%	76%	71%
European institutions	Do not Trust	22%		
	Trust	78%		
Banks and financial institutions	Do not Trust			
	Trust			
Health and medical institutions	Do not Trust		16%	23%
	Trust		84%	77%
Shops and department stores	Do not Trust	45%	60%	51%
	Trust	55%	40%	49%
Internet companies	Do not Trust	55%	67%	57%
	Trust	45%	33%	43%
Phone companies, mobile phone companies and ISPs	Do not Trust	51%	62%	54%
	Trust	49%	38%	46%

Base: SC users.

Source: QB25.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Table 92. Approval required for personal data handling, concern abut re-use of personal information and medical information disclosed

		Medical information		
		Disclosed (self-revealing)	Not disclosed	
			Personal (cautious)	Not Personal (indifferent)
Approval required	Yes, in all cases	61%	74%	68%
	Yes, in the context of personal information asked on the Internet	29%	17%	
	Yes, in the case of sensitive information (health, religion, political beliefs, etc.)			
	No		3%	5%
Concern about re-use	Total 'Concerned' about re-use	75%	70%	66%
	Total 'Not concerned' about re-use	25%	29%	34%

Base: SC users.

Source: QB24, QB26.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

of trust is lower, self-revealing individuals are more likely to trust shops and department stores (55%) and phone companies (49%) and Internet companies (45%) than cautious (40%, 38% and 33% respectively) and indifferent (49%, 46% and 43% respectively). These results are strikingly similar to those reported in Table 80.

In line with this finding, SC users who disclose medical information are also slightly less likely to consider that specific approval is required before personal information is collected and processed [Table 92]. However, in the context of personal information asked on the Internet these individuals are more likely to consider specific approval. Also, they are more likely to be concerned about the re-use of personal data for different purposes (75% self-revealing – 70% cautious – 66% indifferent). Thus, again, context makes a difference to people's attitudes, in this case concern grows as we move closer to actual experience of SC users. In this case, percentage of individuals who considered medical information as personal and stated that specific approval should be required in all cases (76%) is lower than the percentages of self-revealing individuals (61%) while concern about re-use is strikingly similar

5.8.2 Control: deletion of personal data and portability

Respondents who had disclosed personal information on SC sites were asked how much control they felt they had over the information they had disclosed, such as the ability to amend, delete or correct this information.[92] Perception of control does not vary significantly whether SC user disclosed or not medical information. Nevertheless SC users who did not disclose medical information and did not consider it as personal (indifferent) are slightly more likely to feel they have control over the information than cautious users [Table 93].

92 QB6a How much control do you feel you have over the information you have disclosed on social networking sites and\ or sharing sites, e.g. the ability to change, delete or correct this information?

Table 93. Control and medical information disclosed in SC sites

	Total SC users	Medical information		
		Disclosed (self-revealing)	Not disclosed	
			Personal (cautious)	Not Personal (indifferent)
Complete control	27%		26%	30%
Partial control	53%		53%	54%
No control at all	20%		22%	17%

Base: SC users.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Source: QB6a.

Table 94. Possibility to delete personal data held by controllers, data portability and medical information disclosed

		Medical information		
		Disclosed (self-revealing)	Not disclosed	
			Personal (cautious)	Not Personal (indifferent)
Data deletion	Whenever you decide to delete it	63%	79%	71%
	When you change your Internet provider	23%		11%
	When you stop using the service\ website	21%	27%	20%
	Never	6%	2%	6%
Data portability	Very important	28%	34%	31%
	Fairly important	56%	41%	49%
	Not very important	10%	17%	15%
	Not at all important		7%	5%

Base: SC users.

Source: QB28, QB29.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

SC users who do not disclose medical information are more likely to state that they would like their personal data to be completely deleted whenever they decide it (79% cautious; 71% indifferent vs. 63% self-revealing). On the other hand, self-revealing individuals are more likely to want to have the possibility to delete personal data when they change Internet provider (23% self-revealing vs. 11% indifferent) [Table 94]. In accordance with these results, self-revealing individuals are more likely to consider data portability important (84%) than cautious individuals (75%) and indifferent individuals (80%)

5.9 Awareness, identity theft, regulation

SC users who disclose medical information (self-revealing individuals) are more likely to be aware of identity theft (see Table 95) firstly through word of mouth and/or acquaintances

Table 95. Awareness of identity theft and medical information disclosed

	Medical information		
	Disclosed (self-revealing)	Not disclosed	
		Personal (cautious)	Not Personal (indifferent)
Media awareness		49%	37%
Social awareness	33%	23%	
Self-family experience	14%	6%	5%
No	28%	37%	44%

Base: SC users.

Source: QB30.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Table 96. Desire to be informed by controller whenever personal data held is lost or stolen and medical information disclosed

	Medical information		
	Disclosed (self-revealing)	Not disclosed	
		Personal (cautious)	Not Personal (indifferent)
Yes	90%	94%	90%
No	10%	6%	10%

Base: SC users.

Source: QB31.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Table 97. Importance of having same data protection right across Europe and medical information disclosed

	Medical information		
	Disclosed (self-revealing)	Not disclosed	
		Personal (cautious)	Not Personal (indifferent)
Very important	52%	65%	49%
Fairly important	44%	31%	46%
Not very important		3%	4%
Not at all important			

Base: SC users.

Source: QB32.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

(33% social awareness) and secondly through a member of their family and/or themselves (14% Self-family awareness) while it is also likely that they are unaware of identity theft (28%). Conversely, cautious individuals are made aware primarily through the media (49%) and secondarily through social awareness while it is also very likely that they are unaware (37%) of such situations. Similarly, indifferent individuals are more likely to be unaware (44%) and secondarily made aware through the media (37%).

Table 98. Public authority responsible for protecting your rights regarding your personal data and medical information disclosed

	Medical information		
	Disclosed (self-revealing)	Not disclosed	
		Personal (cautious)	Not Personal (indifferent)
Yes	54%	40%	33%
No	46%	60%	67%

Base: SC users.

Source: QB38.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Table 99. Enforcement of the rules on personal data protection and medical information disclosed

	Medical information		
	Disclosed (self-revealing)	Not disclosed	
		Personal (cautious)	Not Personal (indifferent)
European level		52%	48%
National level			
Regional or local level		7%	10%

Base: SC users.

Source: QB37.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

Most SC users (see Table 96) desire to be informed by a public authority or by a private company whenever information they hold about them is lost or stolen. Cautious individuals are slightly more likely to want to be informed (94%) than self-revealing and indifferent individuals (both 90%).

Similar consensus emerged among SC users about the importance of having the same data protection right across the EU (see Table 97): more than 95% of the individuals consider it important. Cautious individuals are more likely to consider it very important (56%) than self-revealing (52%) and indifferent (49%) individuals.[93]

On the other hand, self-revealing individuals (54%) are more likely to be aware of the national authority responsible for protecting their rights regarding personal data than cautious individuals (40%) and indifferent individuals (33%) [Table 98].

Moreover, there is no statistically significant relationship between SC users who disclose medical information and those who do not disclose this type of information in the case of deciding at which level the enforcement of the Data Protection rules should be dealt with (Table 99 European, National or Regional/local).

Finally, all respondents were asked about the need for special protection of genetic data

93 The trends reported in Table 97 and Table 98 are similar for those individuals who considered medical information as personal [5.3].

Table 100. Need for special protection of genetic data as sensitive personal data and medical information disclosed

	Total individuals	Total SC users	Medical information		
			Disclosed (self-revealing)	Not disclosed	
				Personal (cautious)	Not Personal (indifferent)
No, definitely not	2%				
No, not really	5%			4%	6%
Yes, to some extent	25%		38%		32%
Yes, definitely	68%		55%	75%	60%

Base: SC users.

Source: QB33.

Note: Only significant difference at p < 0.01 are reported [i.e. when there is a 99% probability that the relation reported is not due to chance].

as sensitive personal data.[94] Seven out of ten Europeans stated that special protection is needed definitely (68%) and a quarter to some extent (25%). However, self-revealing individuals are less likely to consider that this special protection is needed definitely (55%) than cautious (75%) and indifferent (60%) individuals. In essence this is evidence that self-revealing individuals are not likely to be revealing genetic information while sharing information over Social networks.

5.10 Self-protection

The survey also asked various questions concerning self-protection of one's data online. Specifically, it asked questions in relation to changing one's profile privacy settings on SC sites[95] and questions concerning a range of practical measure to minimise risks related to personal data disclosure (e.g. minimisation, withholding, adjusting, software, etc…).

Overall, more than half of SC users has tried to change privacy settings (51%), while almost half has not (46%). This implies a significant degree of trust of users in the default setting of such site for all SC users. **Self-revealing** SC users are slightly less likely to try to change privacy settings (48%) than users who do not disclose medical information. However, there is no statistically significant difference regarding whether they had encountered difficulties to change their privacy settings[96] or when queried over other reasons why they did not try to change the privacy settings.[97]

Respondents were finally asked about the steps they were taking to protect their personal data and identity, both online and offline.[98] Concerning Internet protection, a scale was created that ranged from 0 to 8 possible protection behaviours [see fact sheet on Social Networking]. Self-revealing SC users are no more likely to stay protected online; conversely, cautious individuals are more likely to do so (r = .19) while indifferent SC users

94 QB33. EU data protection rules nowadays provide for special protection for the processing of sensitive personal data, such as data related to health, sex life, ethnic origin, religious beliefs, political opinions, etc. Do you think that genetic information such as DNA data should also have the same special protection?

95 QB10a Have you ever tried to change the privacy settings of your personal profile from the default settings on a social networking site and/ or sharing site?

96 QB11a How easy or difficult did you find it to change the privacy settings of your personal profile?

97 QB12a Why did you not try to change these privacy settings?

98 QB15. In your daily life, what do you do to protect your identity? Please indicate all that apply in the following list. QB16. And, specifically on the Internet, what do you do to protect your identity? Please indicate all that apply in the following list.

were less likely to protect themselves online (r = -.19). Similar results were found concerning overall management of one's personal data, with cautious users more likely not to disclose and to adjust the personal information they provided (r correlations in the order of .2), and indifferent users less likely to do so (similar r coefficients with negative sign). Overall, the difference in self-protection behaviour, similarly to the results found for perceptions of the SC environment reported above, is marked more by the consideration of one's health information as personal or otherwise than by actually having disclosed medical information on SC sites.

6 Conclusions

6.1 Electronic commerce

1 eCommerce is becoming mainstream in Europe as about 40% of all EU27 citizens engage in this activity (60% of all Internet users). But the bulk of eCommerce occurs within Member States (46% of all Internet users); there are very limited online purchases cross border and very little difference between percentages of people buying inside and outside the EU (18% and 13% respectively). Notable is the relation between different locations of eCommerce: virtually nobody shops in-EU and out-EU without shopping in their own country. This finding is important per se and in relation to disclosure in eCommerce.

2 The uneven take-up of eCommerce in MS is striking; it ranges from Denmark and the Netherlands (81% of Internet user) to Bulgaria (21%) and Portugal (22%). At country level, there is a strong correlation between Internet use and proportion of people shopping online; this should not necessarily be the case. There appear to be two Europes: one at a lower level of eCommerce, and the other at a higher plateau. For both blocks there is an almost perfect correlation between Internet use and eCommerce. This we interpret to mean that there are national factors that influence eCommerce uptake – supply, structure of the digital market, regulation [not higher perception of risk, according to our data]; but also that Internet use and eCommerce have common roots, namely that the socio-economics underpinning Internet uptake [affluence, education, age], also strongly influence online shopping.

3 eCommerce activities are most similar to other 'transactional' activities, generally carried out within one's own country – home banking and eGovernment. It may well be that eServices are a 'single bundle' in people's eyes and experience, but they are MS-based. People shopping online in their own countries also tend to do home banking and eGovernment, while people who shop in the EU and outside the EU tend to do that only. Also, frequent Internet users shop slightly more across borders; the strongest predictor is the overall number of Internet activities carried out. This may mean that the three activities may grow together only if interoperable systems are provided that make it easier to transact outside one's own country; the question remains open whether eCommerce could assist eGovernment, which is currently very low in EU27 [23% of Internet users].

4 In eCommerce, there is a common core of disclosure of name and address [about 90%], and to lesser extent nationality and mobile number [about 40%]. There are four main types of information people disclose 'jointly': biographical information [often disclosed], social information [never disclosed], sensitive information [seldom disclosed] and security-related information [sometimes disclosed]. Financial information does not belong in the security group, but in the sensitive information group. This pattern of behaviour may be good news for those wishing to create a disclosure system based on third-party credentials, rather than on direct disclosure of bank or credit related information.

5 Very few people share their social activities in the context of eCommerce; as this information is not normally asked by eCommerce sites, the low number

is understandable. People share their activities elsewhere, such as in Social Networking Sites; advertising seems to be an increasingly important selling point for SNS and an important source of revenue. This may also mean that traditional eCommerce vendors may have been less rapid than SNS companies to see the value of web2.0 for offering to customers products [generally digital, such as music, but not only] tailored to and anticipating their preferences. If this is the case, which need to be further probed by a market survey, then again European eCommerce companies and sites [which are where most people buy] may be at a competitive disadvantage vis-à-vis largely US-owned SNS sites.

6 The similarity between MS in relation to personal disclosure of 'biographical data' is truly remarkable; this may allow for significant harmonisation and, should problems exist (and they do exist, we argued in point 3), be addressed across EU27 by either technical (identity by design, credential cores) or legal means (harmonisation, standards). But there are differences across regional blocks for other personal data, such as mobile phone and nationality, in particular, and security-related information in general. Increasingly, eCommerce sites make use of authentication techniques based on identity number, mobile number (via SMS) and other ways of pegging 'virtual identity' to real identity. This type of disclosure (security-related) is highest in countries with established systems of electronic authentication (Austria, Belgium, Spain, Finland, The Netherlands and Sweden). Possibly, there is a case for extending this practice to other countries, and to other possible credentials (such as name and address), via burgeoning effort of identity credentials, which may well work cross-borders.

7 Disclosure behaviour is related to other Internet behaviours, rather more strongly than it is related to attitudes towards disclosure. That is: the steering of certain desired behaviours in terms of disclosure depends more on 'behavioural' remedies and tools than with greater awareness and enhanced perceptions, especially of risks. Specifically, people who disclose biographical information also use credentials such as credit cards and customer cards in their daily lives, and they are also more likely to stay protected online using a range of strategies. But these credentials are also much less strongly associated with the disclosure of sensitive information and security information. People who disclose more biographical information also minimise what they disclose and adjust the information according to context as coping strategies in daily life, online and offline. Provision of security information is also to some extent adjusted to context. This may be good news for enforcing the principles of data minimisation or purpose-binding.

8 Overall, there is no apparent relation between considering one's data personal and disclosing it on eCommerce sites. So even if people consider information personal, still they disclose it. Still more surprising, for many items [name, address, nationality, financial information], the more people consider this information personal, the more they disclose it on eCommerce sites [!]. It is true that in order to shop online, some information has to be disclosed, regardless of whether it is considered as personal. But this also may mean that information takes on personal connotation for people when it is disclosed, rather than having 'a priori' personal value. In this case, a system of credentials where no face-value information is disclosed may help people perceive that the information they have disclosed is 'procedural' rather than personal.

9 eCommerce users mention fraud (55%), stealth use of and stealth sharing of one's information with a third party (both at 43%), and identity theft (35%) as major risks of disclosure. Concern about unauthorised reuse of personal data is related to risks of identity theft and fraud, not with risks of unwanted commercial offers of stealth use of data [therefore security rather than profiling risks]. Risks to reputation and to personal safety are mentioned by far fewer respondents. A few correlations also stand out. Those who use government-issues credentials are less likely to fear risk of identity theft; but people using business-related credentials are more likely to fear risk of identity theft. Also, people who fear risks of different nature are also more likely to take active steps to protect their personal identity, both online and offline.

10 People do not quite feel in control in eCommerce. Less than one in five eCommerce users think they have total control on their own information, about one in three thinks they have no control at all, while about half think they have some control. This may be normal, as except for large eCommerce portals, people do not have a profile page available to them, or a single point of entry or a purchase history (what they bought in past interaction, what they searched for, offers looked at). This may make it harder for people to feel in control of personal data they have disclosed one-off, several times on different sites. But control is central to user's eCommerce activity. People who feel in control of their data trust companies and institutions to protect their data; they are less concerned about observation, about re-sue of their data and much more comfortable with online profiling; furthermore, they are far less likely to enjoy disclosing information. Therefore, if eCommerce is to be fostered, one may speculate on the relative merits of alternative solutions: strict data deletion policies, enforcement of the minimisation principle, on the one hand as traditional supply-side rules, and compulsory email notifications of data held, personal data consoles for users to use as demand side enabling tools enhancing control.

11 Individual and companies are seen as being responsible for keeping data safe, rather than policymakers. A minority of eCommerce users (20%) consider public authorities responsible. But about the same proportion (40%), argue that they or companies are responsible to keep their personal data safe. Overall, abut one in two respondents do not see public authorities as having either primary or secondary responsibility for protection of personal data safety. This result is remarkable, as there are small differences in attributing responsibility based on socio-economic traits, as well as on country of residence. People who think they have control on their data tend to see only joint self-company responsibility. In all cases, companies are seen as responsible regardless of level of perceived control [e.g. their conferred responsibility remains relatively stable across perceived control].

12 Results on responsibility are also rather more sobering regarding self-protection. There is no relation between perceptions of self responsibility in eCommerce and most other regulatory perceptions: desire for the possibility to delete one's data, to move one's data and awareness of identity theft and data loss. What is more worrying is that there is no relation between perceived self-responsibility and Internet protection behaviours and very little relation with identity protection behaviours in general. As found in previous surveys, even people feeling responsible do [as little] as the next person to protect their personal data once they have been disclosed. As it was noted above, this may be due to the lack of tools allowing people to take care, effectively if at

all. When tools are available, such as privacy notices, people do read them if they feel responsible. So, all in all, better tools may be required if people have to take care of themselves online.

13 Finally, the picture for responsibility is more complex that the baseline. On the one hand, people who are happy to disclose personal data [about one in four Europeans!] think it is authorities who are responsible, rather than companies. But trust in companies as personal data controllers appears to reduce the perceived need for authorities' responsibility. People considering authorities responsible have heightened concerns about observation, reduced comfort about online profiling and more concern about re-use of their data. In all these cases, people are also slightly more likely to think companies, rather than oneself, are responsible for correct handling of personal data [understandably, as there is little they can do]. This suggests that fostering [genuine] trust in data controllers and their practices may remove part of the burden from regulator's shoulders.

6.2 Social Networking Sites

14 More than a third of all Europeans use SNS (34% of EU27 population). SNS users are more likely to be younger and well educated. They are also heavier Internet users and are still studying or are unemployed. SNS users are as 'green' as generally believed, but they are also able to harness the Internet to a greater extent than previously known: more than half of SNS users also utilised websites to share pictures, videos, movies, etc (68%); instant messaging, chat websites (57%) and have purchased goods or services online (57%).

15 The more the Internet is widespread, the more Internet users also use Social networking sites (SNS); however, age plays a key role at national level. This means that younger people in most EU countries use the Internet very little outside SNS while older people who use SNS are practically the same as the percentage of Internet users. The generation split may be set at 40 years of age as the age group [40-54] tend to act more like the 55+ while the [25-39] more like the [15-24].

16 In general SNS are used the most in Hungary (80%), Latvia (73%), Malta (71%), Ireland (68%), Cyprus, Slovakia (both 66%), Poland and Denmark (both 63%), and least in Germany (37%). When considering usage risks, SNS users living in the north of Europe, specifically Germany, Sweden, France, Ireland and Denmark appear to have more concerns about using SNS; conversely, residents of Italy, Romania, Poland and Portugal, that is mainly the south but also the east of Europe, are likely to perceive lesser risks in SNS activity.

17 Age appears to play the most important role in the type of information that is disclosed by SNS users: social (photos; activities; preferences), sensitive (work history; fingerprints; medical/financial information), or traditional identifiers (address; mobile number; name and nationality). There are no discernible regional patterns concerning overall disclosure which may signal that SNS use is still very national, as people do disclose different types of information on language based-sites or due to country-culture differences or even regulatory framework.

18 People understand they need to disclose social information if they want to socialise online. Overall, there is no apparent relation between considering one's data personal and disclosing it on SNS. The most important reasons for disclosing personal information when using SNS are to access a service (61%) followed by connecting with others (54%). However, more people provide

commercially valuable information on SNS than people provide social information on eCommerce sites; this may point to an advantage of SNS operators over eCommerce providers regarding viability of business plans based on Web2.0 dynamics – extracting monetary value from people's personal information.

19 SNS users are less cautious about sharing their social information [friends, activities, etc.] since they think that disclosure is unavoidable in today's' life, although they consider it personal. SNS users are less concerned to being 'observed' online – more comfortable with online profiling – but more cautious in sharing their sensitive [medical, financial, etc.] information.

20 In some countries, SNS users are slightly more likely to disclose happily [Italy, Estonia], and to think that disclosure is unavoidable. Conversely, in other countries [Greece, Cyprus, Slovenia], people are less likely to be happy to disclose their personal data; they also think that disclosure could be avoided. Unavoidability of disclosure is also related to the benefit of the service related to the data disclosure.

21 The issue of informed consent in SNS is more complicated than may be thought. There are four groups of SNS users in relation to it: 19% of all SNS users claim to have not been informed of either conditions or consequences; 29% report having been informed about conditions of data collection, but are unhappy with the degree of information about possible consequences; 40% have been informed about both collection conditions and consequences; and 11% are happy about SNS sites informing them of consequences, but have hardly been given information on how the data collected will be used. In policy terms, significant work is required to enforce informed consent and enhanced information about what may happen with people's personal data once it is disclosed in SNS.

22 Managers and other white collar workers are mainly using SNS sites that relate to their work history and to relate to friends (peers or even competitors); while still not very diffused this practice seems to be gaining ground with many institutions opening up Facebook–like sites to promote internal communication and cross-fertilisation of ideas.

23 SNS users are less likely than Internet users to use private or government-related credentials, are more likely than Internet users to report to have been informed about data collection conditions when disclosing personal data to access an online service and use a slightly wider range of strategies to protect their personal data online than the average Internet user. This may be due to younger age.

6.3 Identity and authentication in Europe

24 Frequent Internet-users are more likely to use leisure-related credentials: driving license, customer cards, passports and Internet accounts, but less likely to use national identity cards. This points to the increasing embedding of credentials, rather private than public, in the fabric of the Internet. This may only be natural, as government-issued credentials can today be used to carry out online commercial transactions in a limited number of countries only, including Belgium, Austria, Spain and Estonia.

25 A significant proportion of respondents – including SNS and eCommerce users – claim they are not using an Internet account, while they carry out activities that clearly require one; this is not the case of the Digital

Natives. Much work needs to be done raising awareness of Internet users regarding the identity-related personal data they routinely provide to online service providers via their accounts, without being aware.

26 The system of credentials is highly fragmented in Europe: by country, by socio-economic status and by Internet use. Overall, differences in the use of credentials are not necessarily regional or related to economic growth and macro-economic indicators, but they mirror the structure of credentials in place in single countries. The use of identity cards varies greatly: respondents from the east and south of the European Union are more likely to use them than those living in the north and west. There are no such differences in the use of passports. Trust alone makes only a little difference in the likelihood of having a bank / credit card. Conversely, controlling for trust, country of residence makes a large difference [e.g. +21% for people living in Sweden, and -44% for residents of Greece]. Social position and younger age make a difference. For Internet users, use of business-related credentials is strongly associated with online transactions such as home banking, eGovernment and ecommerce; but it is inversely related with online social activities. Internet behaviour is unrelated to the use of government-related credentials. This fragmentation may not bode well for the adoption of cross-border eGovernment and cross-border eCommerce, even where Internet access should become more widespread and faster.

27 People who use business-related credentials are more likely to report slightly higher perception of risk of identity theft and fraud due to eCommerce disclosure; conversely, people using government related credentials are likely to report reduced perception of risk of identity theft in eCommerce. This may be natural: people are likely to associate higher risks to the loss of financial rather than governed-related information as it constitutes to them a greater and more visible asset. Those who use credentials of both types are more likely to trust institutions as data controllers, especially business-related credentials; those who do not trust companies as data controllers are likely to make greater use of government-related credentials. Therefore, use of credentials may be enhanced by portability of trust from public institutions to commercial institutions, via the greater use of government-supported, if not issued outright, credentials, or by establishing circles of trust through Public-Private-Partnerships (PPP).

28 There are significant national differences in the relation between disclosure in eCommerce and use of credentials; in other words, what credentials people use as they transact online. Overall, the structure of disclosure in eCommerce is dominated by privately-released credentials: credit cards and customer cards; government cards and identity cards only have a marginal role in the structure of disclosure. However, in some countries where the structure of electronic authentication is most advanced [Austria, Belgium, Germany] people use government-related and business-related credential in relation to eCommerce disclosure. Again, the former credentials are usually associated with lower level of disclosure of sensitive information. In some countries, government related credentials are dominant [Spain, Sweden and Poland], while in some countries business credentials underpin most of people's disclosure in eCommerce [UK, Ireland, Italy and Estonia]. These findings largely resound with industry-level analysis on the structure of the electronic identity market in Europe.

29 Concerning regulation, users of business-related credential are strongly in favour of homogeneous data protection right across EU, to be informed when their personal data

is lost or stolen, and to be able to edit/delete their data whenever they wish so. On the one hand, this hints that 'if you build it they will come': engaging people in safer online authentication may get them to value their personal data more, and be more willing to protect them [see par. 32]. But it also appears that remedies requiring more of people's initiative are less popular than institution-centred remedies.

30 Personal experience of identity theft and data loss is very low in Europe, affecting only 2% of EU27 population. For the sake of comparison, identity theft only [but not data loss], affected about 3.5 % of US residents in 2010. Largely, identity theft and data loss affect managers and other office workers and their families; people with customer cards are more likely to have reported incidence of identity theft and data loss [6%]; the reverse is true for holders of national identity cards [8% of non-holders]. Internet users are more likely to report overall awareness, media awareness and experience with the phenomenon [incidence is three times higher for heavy internet users].

31 Sensitivity to identity theft and data loss is relatively high, as more than half are aware of the issue via different or multiple sources, which increases to two in three in most northern countries, where Internet access is higher. Thus, general Internet skills alone do not provide an answer to identity theft and data loss, and other more specific skills may be needed [see par. 34]. Also, concerning remedies, media awareness appears intertwined with calls for enhanced regulation, including greater harmonisation of data protection rights across EU27, request for information if/when data lost or stolen and the possibility to delete personal data. The media may thus be playing a role in generating support for a more vigorous and more articulated response to the challenge.

32 While a majority of Europeans take one or more actions to protect their personal identity data [average is 2.3 actions], a significant minority do not minimise disclosure, do not withhold bank details, they provide information to controllers they do not trust and disclose usernames and passwords. All in all, this is in line with the widespread perception that disclosure is unavoidable. However, lack of protection is not caused by resignation: if you think disclosure is unavoidable you are slightly more likely to protect yourself. Rather it is strongly linked to propensity to disclose personal data, which one in three Europeans happily does. Specifically, those who are happy disclosing personal data, those who trust companies [!!] and those comfortable with online profiling are much less likely to minimise data, as may be obvious, but are also less likely to withhold sensitive information and to use software measures to protect their data.

33 Personal data protection is particularly low in southern European countries, eastern and central European countries, and relatively high in Scandinavian countries and the Netherlands. In fact, people use very different strategies across Member States. Offline, traditional strategies are linked to high concern about observation, while minimisation is linked to Internet use, especially eCommerce. So while people in Nordic countries are generally less concerned about their behaviour being recorded, and are more likely to use eCommerce [and thus minimise], the situation is inverse for other countries mentioned. Thus use of the Internet for transactions may have a beneficial awareness-raising effect. Also, media awareness of identity theft and data loss is particularly important to make people minimise personal data disclosure.

34 Internet users use a different mix of strategies to protect themselves, possibly as they have to face a different challenge, largely

related to risks of online fraud and identity theft. Rather than minimisation and low-tech strategies, a majority of Internet users engage in security-enhancing, information withholding behaviours. Particularly, those who use business-related credentials, often in eCommerce, are much more likely to try to minimise the information they disclose. Also, Internet users engaging in online transactions are much more likely than ordinary internet users to take a range of measure to protect their data online, including data minimisation and reactive software use. This confirms the intuitive idea that being on the Internet hones specific strategies of self protection than carrying oneself in offline, everyday life.

35 But what was reported in par. 33 does not mean that Internet users actually protect themselves to a sufficient degree. On the Internet, protection behaviour rests on passive use of existing tools [e.g. tools and strategies to limit unwanted emails – 40%] rather than on active strategies of information control [e.g. changing the security settings of your browser – 22%]. There is a strong correlation between the overall number of internet activities carried out [a proxy for internet skills], and online protection behaviour. But also, people in some countries tend to stand more protected online regardless of the number of activities they carry out on the Internet. These deviations from the trend hint at the importance of variables others than internet use to explain protection; these may have to do with national technical culture and with maturity of the market for online protection tools. This all implies that where simple tools are not available, or are cumbersome to use for the average user, people are unlikely to take proper care of their personal identity data online.

36 Data minimisation is strongly correlated with regulatory preferences and data protection principles. In short, people who minimise the information they disclose also tend to have particularly strong feelings regarding the needs for stronger protection of their rights in EU27 and on enhanced control of their personal data, such as deletion on demand and data breach notification. Also, existing rules and principles of data protection engender greater self-protection by Internet users. Namely, those who think they had to disclose more that they wished actually did so compensated by using reactive, proactive and deception strategies. Information about data collection conditions is associated positively with reactive and proactive behaviour and with minimisation. Finally, concern about re-use of one's data is associated with significant minimisation of the data disclosed.

6.4 Medical information as personal data

37 Around three-quarters of Europeans think that medical information such as patient records and health information (74%) is personal. Thus, Health information, financial information and national identity information are equally perceived to be personal.

38 There are only small socio-economic differences in the perception of medical data as personal between well educated, white collar, wealthy respondents [more likely to say it is personal], and those with lower education, outside the labour market and less wealthy.

39 There are significant country differences in the perception of medical information as personal; respondents located in the north and west of the European Union are most likely to regard medical information as personal. In the south east the situation is different, especially in Poland (46%), Portugal and Romania (each 50%) and Bulgaria (52%). In these countries,

identity credentials, such as identity cards and passports, are deemed to be personal over and above sensitive information (financial, medical).

40 Considering medical data as personal makes a large difference to a range of regulatory preferences. Those who consider medical information as personal are more likely to want to be informed whenever information held about them is lost or stolen (91% vs. 78%) and to desire the same protection over their personal information regardless of the EU country in which it is collected and processed (79% vs. 57%).

41 People who consider medical information as personal are more likely to be concerned about stealth re-use of their personal data than individuals who did not consider it personal, regardless of whether they trust or not data controllers. But trust in data controllers is a powerful mediating factor. Trust in public institutions significantly reduces the worry of those who care about their medical data. And trust in shops, Internet and phone companies is extremely important, almost critical, as it is associated with significantly lower concerns across the sample, for both people who consider medical data as personal and otherwise.

42 Although a majority of people consider that medical information is personal, still a small percentage do disclose it – medical information is disclosed in the context of eCommerce (3%) and Social networking (5%). They are aware of the risks involved and still they do it; it can only mean that they are getting a benefit from the disclosure or are obliged to do it.

43 There are three groups of Europeans concerning medical information disclosure in the context of Social Computing. "**Self-revealing**" social computing users disclose medical information (5%). "**Cautious**" users consider medical information as personal and do not disclose (73%). "**Indifferent**" neither consider it as personal nor do they disclose it (22%). These three groups consist of Internet users who are also users of social computing sites – thus largely users who are better educated and in a better socio-economic status than non-Internet users – who however, are statistically different in many other respects.

44 Cautious users are slightly more likely to be female (51% vs. 49%) while indifferent individuals are more likely to be male (56% vs. 44%); this characteristic points out the importance of women in relation to health issues.

45 Self-revealing individuals are more likely to be older than cautious and indifferent individuals (this profile is the youngest one), probably because older individuals are more likely to either face a health problems themselves or care for someone else in the family. Although due to age, self-revealing users are also less educated than cautious or indifferent individuals, their overall high education makes the risk of health illiteracy minimal, especially if we compare these individuals with non internet users. Due to the active participation of this typology of Internet users as regards their health, health information on the internet has a higher potential to empower individuals, with a positive impact on health outcomes.

46 Self-revealing individuals who also are Internet users are more likely to be using the Internet in more sophisticated ways; cautious users carry out more eCommerce and eGovernment transactions – which may be the reason they are indeed cautious; while indifferent Social Computing site users are less likely to do either (that is, they largely carry out ordinary Internet activities, email and search).

47 Self-revealing individuals share information for very specific reasons, namely: (a) to connect with others – one would think similar individuals; (b) so as to get a service for free – in relation to their condition; and (c) to save time at the next visit – presumably when receiving a service over time.

Annex: Survey Questionnaire

Legend

DK = don't know/no answer – always spontaneous
(OUR COUNTRY) will be replaced by the name of the country in each country
(NATIONALITY) will be replaced by the nationality of the country in each country

Socio-demographic variables

Q1 is the initial question about nationality
D1 – Left/right political scale
D7 – Marital status of the respondent
D8 – Age of end of education of the respondent
D10 – Gender of the respondent
D11 – Age of the respondent
D25 – Subjective urbanisation
D40 – Household composition
D43a – Landline phone in the household
D43b – Personal mobile phone
D46 – Equipments in the household
D60 – Difficulties in paying bills
D61 – Self-positioning on the social scale

ASK D15b IF "NOT DOING ANY PAID WORK CURRENTLY", CODES 1 to 4 in D15a

D15a What is your current occupation?
D15b Did you do any paid work in the past? What was your last occupation?

	D15a CURRENT OCCUPATION	D15b LAST OCCUPATION
NON-ACTIVE		
Responsible for ordinary shopping and looking after the home, or without any current occupation, not working	1	
Student	2	
Unemployed or temporarily not working	3	
Retired or unable to work through illness	4	
SELF EMPLOYED		
Farmer	5	5
Fisherman	6	6
Professional (lawyer, medical practitioner, accountant, architect, etc.)	7	7
Owner of a shop, craftsmen, other self-employed person	8	8
Business proprietors, owner (full or partner) of a company	9	9
EMPLOYED		
Employed professional (employed doctor, lawyer, accountant, architect)	10	10
General management, director or top management (managing directors, director general, other director)	11	11
Middle management, other management (department head, junior manager, teacher, technician)	12	12
Employed position, working mainly at a desk	13	13
Employed position, not at a desk but travelling (salesmen, driver, etc.)	14	14
Employed position, not at a desk, but in a service job (hospital, restaurant, police, fireman, etc.)	15	15
Supervisor	16	16
Skilled manual worker	17	17
Other (unskilled) manual worker, servant	18	18
Never did any paid work		19

D62 Could you tell me if…?
(SHOW CARD WITH SCALE – ONE ANSWER PER LINE)

	(READ OUT)	Everyday\ Almost everyday	Two or three times a week	About once a week	Two or three times a month	Less often	Never	No Internet access (SPONTANEOUS)
1	You use the Internet at home, in your home	1	2	3	4	5	6	7
2	You use the Internet on your place of work	1	2	3	4	5	6	7
3	You use the Internet somewhere else (school, university, cyber-café, etc.)	1	2	3	4	5	6	7

ASK QB1a AND QB1b IF "USE THE INTERNET", CODE 1 TO 5 IN D62.1 OR D62.2 OR D62.3 – OTHERS GO TO QB2

QB1a For each of the following activities, please tell me if it is an activity that you do, or not, on the Internet.
(ONE ANSWER PER LINE)

	(READ OUT)	Yes	No	DK
1	Use websites to share pictures, videos, movies, etc.	1	2	3
2	Use a social networking site	1	2	3
3	Purchase goods or services online\ online shopping (e.g. travel & holiday, clothes, books, tickets, films, music, software, food)	1	2	3

QB1b Which of the following activities do you also do on the Internet?
(SHOW CARD – READ OUT – ROTATE – MULTIPLE ANSWERS POSSIBLE)

Keep a blog (also known as web-log)	1,
Instant messaging, chat websites	2,
Use peer-to-peer software and\ or sites to exchange movies, music, etc.	3,
Make or receive phone calls or video calls over the Internet	4,
Install plug-ins in your browser to extend its capability	5,
Design or maintain a website (not just a blog)	6,
Do home banking	7,
(ONLY IF "YES" IN QB1a.3) Purchase goods or services from a seller located in (OUR COUNTRY)	8,
(ONLY IF "YES" IN QB1a.3) Purchase goods or services from a seller located in another EU country	9,
(ONLY IF "YES" IN QB1a.3) Purchase goods or services from a seller located outside the EU	10,
Submit tax declaration or use other online government services	11,
Use online softwares	12,
Other (SPONTANEOUS)	13,
DK	14,

ASK ALL

QB2 Which of the following types of information and data that are related to you do you consider as personal?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Medical information (patient record, health information)	1,
Your fingerprints	2,
Financial information (e. g salary, bank details, credit record)	3,
Your work history	4,
Your national identity number (USE APPROPRIATE TERM IN EACH COUNTRY)\ card number\ passport number	5,
Your name	6,
Your home address	7,
Your nationality	8,
Things you do (e.g. hobbies, sports, places you go)	9,
Your tastes and opinions	10,
Photos of you	11,
Who your friends are	12,
Websites you visit	13,
Your mobile phone number	14,
Other (SPONTANEOUS)	15,
None (SPONTANEOUS)	16,
DK	17,

QB3 For each of the following statements, could you please tell me whether you totally agree, tend to agree, tend to disagree or totally disagree?

(SHOW CARD WITH SCALE – ONE ANSWER PER LINE)

	(READ OUT – ROTATE)	Totally agree	Tend to agree	Tend to disagree	Totally disagree	Not applicable (SPONTANEOUS)	DK
1	Nowadays you need to log into several systems using several usernames and passwords	1	2	3	4	5	6
2	The (NATIONALITY) Government asks you for more and more personal information	1	2	3	4	5	6
3	You feel obliged to disclose personal information on the Internet	1	2	3	4	5	6
4	There is no alternative than to disclose personal information if one wants to obtain products or services	1	2	3	4	5	6
5	Disclosing personal information is not a big issue for you	1	2	3	4	5	6
6	Disclosing personal information is an increasing part of modern life	1	2	3	4	5	6
7	You don't mind disclosing personal information in return for free services online (e.g. free email adress)	1	2	3	4	5	6

Social networking sites and sharing sites

ASK QB4a TO QB12a IF "USE SOCIAL NETWORKING SITES AND\ OR SHARING SITES", CODE 1 IN QB1a.1 OR QB1a.2 – OTHERS GO TO QB4b

Social networking sites and sharing sites are becoming more and more popular. On these sites, people keep in touch with their friends and families, conduct business, meet new friends or play games.

QB4a Thinking of your usage of social networking sites and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Medical information (patient record, health information)	1,
Your fingerprints	2,
Financial information (e. g salary, bank details, credit record)	3,
Your work history	4,
Your national identity number (USE APPROPRIATE TERM IN EACH COUNTRY)\ card number\ passport number	5,
Your name	6,
Your home address	7,
Your nationality	8,
Things you do (e.g. hobbies, sports, places you go)	9,
Your tastes and opinions	10,
Photos of you	11,
Who your friends are	12,
Websites you visit	13,
Your mobile phone number	14,
Other (SPONTANEOUS)	15,
None (SPONTANEOUS)	16,
DK	17,

ASK QB5a AND QB6a IF "HAVE DISCLOSED PERSONAL INFORMATION ON SOCIAL NETWORKING SITES AND\ OR SHARING SITES", CODE 1 TO 15 IN QB4a – OTHERS GO TO QB7a

QB5a What are the most important reasons why you disclose such information on social networking sites and\ or sharing sites?

(SHOW CARD – READ OUT – MAX. 3 ANSWERS)

To access the service	1,
To save time at the next visit	2,
To receive money or price reductions	3,
To benefit from personalised commercial offers	4,
To get a service for free	5,
To obtain a service adapted to your needs	6,
For fun	7,
To connect with others	8,
Other (SPONTANEOUS)	9,
DK	10,

QB6a **How much control do you feel you have over the information you have disclosed on social networking sites and\ or sharing sites, e.g. the ability to change, delete or correct this information?**

(READ OUT – ONE ANSWER ONLY)

Complete control	1
Partial control	2
No control at all	3
DK	4

ASK QB7a TO QB12a IF "USE SOCIAL NETWORKING SITES AND\ OR SHARING SITES", CODE 1 IN QB1a.1 OR QB1a.2 – OTHERS GO TO QB4b

QB7a **I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of personal information on social networking sites and\ or sharing sites?**

(SHOW CARD – READ OUT – ROTATE – MAX. 3 ANSWERS)

Your information being used without your knowledge	1,
Your information being shared with third parties without your agreement	2,
Your information being used to send you unwanted commercial offers	3,
Your views and behaviours being misunderstood	4,
Your identity being at risk of theft online	5,
Your personal safety being at risk	6,
Yourself being victim of fraud	7,
Yourself being discriminated against (e.g. in job selection, receiving price increases, getting no access to a service)	8,
Your reputation being damaged	9,
Your information being used in different contexts from the ones where you disclosed it	10,
Other (SPONTANEOUS)	11,
None (SPONTANEOUS)	12,
DK	13,

QB8a **Please tell me whether you agree or disagree with the following statement: Social networking sites and\ or sharing sites sufficiently inform their users about the possible consequences of disclosing personal information.**

(READ OUT – ONE ANSWER ONLY)

Totally agree	1
Tend to agree	2
Tend to disagree	3
Totally disagree	4
DK	5

QB9a1 Who do you think should make sure that your information is collected, stored and exchanged safely on social networking sites and\ or sharing sites? Firstly?
QB9a2 And secondly?

(SHOW CARD – ONE ANSWER PER COLUMN)

(READ OUT)	QB9a1 FIRSTLY	QB9a2 SECONDLY
You – as you need to take care of your information	1	1
The social networking sites and\ or sharing sites you are dealing with – as they need to ensure they process your information fairly	2	2
Public authorities – as they need to ensure that citizens are protected	3	3
Other (SPONTANEOUS)	4	4
DK	5	5

A personal profile on a social networking site or sharing site is made of information such as your age, location, interests, an uploaded photo and an "about me" section. Profile visibility – who can see your information and interact with you - can in some cases be personalised by managing the privacy settings offered by the site.

QB10a Have you ever tried to change the privacy settings of your personal profile from the default settings on a social networking site and\ or sharing site?

Yes	1
No	2
DK	3

ASK QB11a IF "YES", CODE 1 IN QB10a – OTHERS GO TO QB12a

QB11a How easy or difficult did you find it to change the privacy settings of your personal profile?

(READ OUT – ONE ANSWER ONLY)

Very easy	1
Fairly easy	2
Fairly difficult	3
Very difficult	4
DK	5

ASK QB12a IF "NO", CODE 2 IN QB10a – OTHERS GO TO QB4b

QB12a Why did you not try to change these privacy settings?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

You did not know that you could change the settings	1,
You do not know how to proceed to change these settings	2,
You trust the site to set appropriate privacy settings	3,
You are not worried by having personal data on social networking and\ or sharing sites	4,
You did not find the time to look at the available options	5,
Other (SPONTANEOUS)	6,
DK	7,

Online shopping sites

ASK QB4b TO QB8b IF "PURCHASE GOODS OR SERVICES ONLINE", CODE 1 IN QB1a.3 – OTHERS GO TO QB13

It is increasingly common to purchase goods and services via the Internet (online shopping). People buy clothes, sports goods, books, travel tickets and holidays online; they purchase films, music and games; they compare prices of goods and services; they buy shares and financial and insurance products.

QB4b Thinking of the occasions when you have purchased goods or services via the Internet, which of the following types of information have you already disclosed?
(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Medical information (patient record, health information)	1,
Your fingerprints	2,
Financial information (e. g salary, bank details, credit record)	3,
Your work history	4,
Your national identity number (USE APPROPRIATE TERM IN EACH COUNTRY)\ card number\ passport number	5,
Your name	6,
Your home address	7,
Your nationality	8,
Things you do (e.g. hobbies, sports, places you go)	9,
Your tastes and opinions	10,
Photos of you	11,
Who your friends are	12,
Websites you visit	13,
Your mobile phone number	14,
Other (SPONTANEOUS)	15,
None (SPONTANEOUS)	16,
DK	17,

ASK QB5b AND QB6b IF "HAVE DISCLOSED PERSONAL INFORMATION WHEN SHOPPING ONLINE", CODE 1 TO 15 IN QB4b – OTHERS GO TO QB8b

QB5b What are the most important reasons why you disclose such information in online shopping?
(SHOW CARD – READ OUT – MAX. 3 ANSWERS)

To access the service	1,
To save time at the next visit	2,
To receive money or price reductions	3,
To benefit from personalised commercial offers	4,
To get a service for free	5,
To obtain a service adapted to your needs	6,
For fun	7,
To connect with others	8,
Other (SPONTANEOUS)	9,
DK	10,

QB6b How much control do you feel you have over the information you have disclosed when shopping online, e.g. the ability to change, delete or correct this information?

(READ OUT – ONE ANSWER ONLY)

Complete control	1
Partial control	2
No control at all	3
DK	4

ASK QB7b TO QB8b IF "PURCHASE GOODS OR SERVICES ONLINE", CODE 1 IN QB1a.3 – OTHERS GO TO QB13

QB7b I will read out a list of potential risks. According to you, what are the most important risks connected with disclosure of your personal information to buy goods or services via the Internet?

(SHOW CARD – READ OUT – ROTATE – MAX. 3 ANSWERS)

Your information being used without your knowledge	1,
Your information being shared with third parties without your agreement	2,
Your information being used to send you unwanted commercial offers	3,
Your views and behaviours being misunderstood	4,
Your identity being at risk of theft online	5,
Your personal safety being at risk	6,
Yourself being victim of fraud	7,
Yourself being discriminated against (e.g. in a job selection, receiving price increases, getting no access to a service)	8,
Your reputation being damaged	9,
Your information being used in different contexts from the ones where you disclosed it	10,
Other (SPONTANEOUS)	11,
None (SPONTANEOUS)	12,
DK	13,

QB8b1 Who do you think should make sure that your information is collected, stored and exchanged safely when you buy goods or services via the Internet? Firstly?

QB8b2 And secondly?

(SHOW CARD – ONE ANSWER PER COLUMN)

(READ OUT)	QB8b1 FIRSTLY	QB8b2 SECONDLY
You – as you need to take care of your information	1	1
The online shopping sites – as they need to ensure they process your information fairly	2	2
Public authorities – as they need to ensure that citizens are protected	3	3
Other (SPONTANEOUS)	4	4
DK	5	5

End of scenarios

ASK ALL

QB13 Nowadays, cameras, cards and websites record your behaviour, for a range of reasons. Are you very concerned, fairly concerned, not very concerned or not at all concerned about your behaviour being recorded…?

(SHOW CARD WITH SCALE – ONE ANSWER PER LINE)

	(READ OUT)	Very concerned	Fairly concerned	Not very concerned	Not at all concerned	Not applicable (SPONTANEOUS)	DK
1	On the Internet (browsing, downloading files, accessing content online)	1	2	3	4	5	6
2	In a public space (street, subway, airport, etc.)	1	2	3	4	5	6
3	In a private space (restaurant, bar, club, office, etc.)	1	2	3	4	5	6
4	Via mobile phone\ mobile Internet (call content, geo-location)	1	2	3	4	5	6
5	Via payment cards (location and spending)	1	2	3	4	5	6
6	Via store or loyalty cards (preferences and consumption, patterns, etc.)	1	2	3	4	5	6

QB14 Which of the following do you currently use?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Credit cards and bank cards	1,
Customer cards (loyalty cards, frequent flyer cards)	2,
National identity cards\ residence permit	3,
Passport	4,
Government entitlement cards (USE APPROPRIATE NAME IN EACH COUNTRY – e. g. BE : carte SIS, FR : carte VITAL)	5,
Driving licence	6,
(ONLY IF STUDENT) Student card	7,
(ONLY IF USE THE INTERNET) An account you use on the Internet (email, social networking, commercial services)	8,
None (SPONTANEOUS)	9,
DK	10,

QB15 In your daily life, what do you do to protect your identity? Please indicate all that apply in the following list.

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Use cash instead of recorded transactions (bank cards, transfers)	1,
Give the minimum required information	2,
Adjust the information you disclose to different contexts (e.g., depending on whether you are dealing with a company, a bank or a website)	3,
Provide wrong information	4,

Disclose information only to people\ organisations you trust	5,
Shred old bills, bank statements, credit card receipts, etc.	6,
Do not disclose payment card details online	7,
Do not disclose your user names and passwords	8,
Do not disclose your bank details or PIN numbers	9,
Other (SPONTANEOUS)	10,
None (SPONTANEOUS)	11,
DK	12,

ASK QB16 TO QB23 IF "USE THE INTERNET", CODE 1 TO 5 IN D62.1 OR D62.2 OR D62.3 – OTHERS GO TO QB24

QB16 And, specifically on the Internet, what do you do to protect your identity? Please indicate all that apply in the following list.

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Use a dummy email account	1,
Use anti-spy software	2,
Delete cookies	3,
Use tools and strategies to limit unwanted emails (spams)	4,
Check that the transaction is protected or the site has a safety logo\ label	5,
Avoid providing the same information to different sites	6,
Change the security settings of your browser to increase privacy	7,
Use a search engine to maintain awareness of what information circulates about you on the Internet	8,
Ask websites to access the information they hold about you in order to update it or delete it	9,
Other (SPONTANEOUS)	10,
None (SPONTANEOUS)	11,
DK	12,

I am going to ask you a series of questions about how personal information or data is collected, treated, stored and protected by public and private organisations.

QB17 When you intend to become a member of a social networking site or register for a service online, you are usually asked to disclose personal information. In these circumstances, have you been informed about the conditions for the data collection and the further uses of your data?

(READ OUT – ONE ANSWER ONLY)

Always	1
Sometimes	2
Rarely	3
Never	4
Not applicable (SPONTANEOUS)	5
DK	6

On the Internet, privacy statements declare how the personal information users enter online will be used and who will have access to it.

QB18 Thinking about privacy statements on the Internet, which of the following sentences best describes your situation?

(SHOW CARD – READ OUT – ONE ANSWER ONLY)

You usually read and understand them	1
You usually read them but do not fully understand them	2
You usually do not read them	3
You do not know where to find them	4
You ignore them	5
DK	6

ASK QB19 IF "READ THEM", CODE 1 OR 2 IN QB18 – OTHERS GO TO QB20

QB19 Have you adapted your behaviour on the Internet after reading privacy statements? Please choose the sentence that comes closest to your experience.

(SHOW CARD – READ OUT – ONE ANSWER ONLY)

Yes, and you have already decided at least once not to use an online service	1
Yes, and you have been more cautious about the personal information you disclose on the Internet	2
No	3
DK	4

ASK QB20 IF "DON'T READ THEM USUALLY" OR "IGNORE THEM", CODE 3 OR 5 IN QB18 – OTHERS GO TO QB21

QB20 What are the reasons why you usually do not read them or you usually ignore them?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

You think the websites will not honour them anyway	1,
You believe that the law will protect you in any case	2,
It is sufficient for you to see that websites have a privacy policy	3,
DK	4,

ASK QB21 TO QB23 IF "USE THE INTERNET", CODE 1 TO 5 IN D62.1 OR D62.2 OR D62.3 – OTHERS GO TO QB24

QB21 As you may know, some Internet companies are able to provide free search engines or free e-mail accounts thanks to the income they receive from advertisers trying to reach users on their websites. How comfortable are you with the fact that those websites use information about your online activity to tailor advertisements or content to your hobbies and interests?

(READ OUT – ONE ANSWER ONLY)

Very comfortable	1
Fairly comfortable	2
Fairly uncomfortable	3
Very uncomfortable	4
DK	5

QB22 Have you ever been required to provide more personal information than necessary to obtain access to or to use an online service (e.g. when registering for an online game or an online information service, purchasing a good online, opening an account with a social networking site)?

(READ OUT – ONE ANSWER ONLY)

Always	1
Sometimes	2
Rarely	3
Never	4
DK	5

ASK QB23 IF "ALWAYS" OR "SOMETIMES", CODE 1 OR 2 IN QB22 – OTHERS GO TO QB24

QB23How concerned are you about such cases?

(READ OUT – ONE ANSWER ONLY)

Very concerned	1
Fairly concerned	2
Not very concerned	3
Not at all concerned	4
DK	5

ASK ALL

QB24 Should your specific approval be required before any kind of personal information is collected and processed?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Yes, in all cases	1,
Yes, in the context of personal information asked on the Internet	2,
Yes, in the case of sensitive information (health, religion, political beliefs, sexual preferences, etc.)	3,
No	4,
DK	5,

QB25 Different authorities (government departments, local authorities, agencies) and private companies collect and store personal information. To what extent do you trust the following institutions to protect your personal information?

(SHOW CARD WITH SCALE – ONE ANSWER PER LINE)

	(READ OUT)	Totally trust	Tend to trust	Tend not to trust	Do not trust at all	DK
1	National public authorities (e.g. tax authorities, social security authorities)	1	2	3	4	5
2	European institutions (European Commission, European Parliament, etc.)	1	2	3	4	5
3	Banks and financial institutions	1	2	3	4	5
4	Health and medical institutions	1	2	3	4	5
5	Shops and department stores	1	2	3	4	5
6	Internet companies (Search Engines, Social Networking Sites, E-mail Services)	1	2	3	4	5
7	Phone companies, mobile phone companies and Internet Services Providers	1	2	3	4	5

QB26 Companies holding information about you may sometimes use it for a different purpose than the one it was collected for, without informing you (e.g. for direct marketing, targeted online advertising). How concerned are you about this use of your information?

(READ OUT – ONE ANSWER ONLY)

Very concerned	1
Fairly concerned	2
Not very concerned	3
Not at all concerned	4
DK	5

QB27 According to EU data protection rules, you have the right to access your personal information stored by public or private entities, in order to change, block or delete it. EU rules do not specify whether access to personal information should be free of charge. In some EU Member States, you have to pay in order to be granted such access. Would you be prepared to pay to have access?

(SHOW CARD – READ OUT – ONE ANSWER ONLY)

Yes, but only a small amount (e.g. postage or communication costs), less than 2€	1
Yes, up to 20 €	2
Yes, more than 20 €	3
No	4
DK	5

ASK QB28 AND QB29 IF "USE THE INTERNET", CODES 1 TO 5 IN D62.1 OR D62.2 OR D62.3 – OTHERS GO TO QB30

QB28 In what circumstances, if any, would you like personal information stored and collected through a website to be completely deleted?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Whenever you decide to delete it	1,
When you change your Internet provider	2,
When you stop using the service\ website	3,
Never	4,
DK	5,

QB29 When you decide to change providers or stop using a service, how important or not is it for you to be able to transfer personal information that was stored and collected through the website?

(READ OUT – ONE ANSWER ONLY)

Very important	1
Fairly important	2
Not very important	3
Not at all important	4
DK	5

ASK ALL

QB30 In the last 12 months, have you heard about or experienced issues in relation to data losses and identity theft?

(SHOW CARD – READ OUT – MULTIPLE ANSWERS POSSIBLE)

Yes, through television, radio, newspapers, the Internet	1,
Yes, through word of mouth	2,
Yes, it affected one of your acquaintances	3,
Yes, it affected a member of your family	4,
Yes, it affected you directly	5,
Yes, others (SPONTANEOUS)	6,
No	7,
DK	8,

QB31 Would you want to be informed by a public authority or by a private company whenever information they hold about you is lost or stolen?

Yes	1
No	2
DK	3

QB32 How important or not is it for you to have the same rights and protections over your personal information regardless of the EU country in which it is collected and processed?

(READ OUT – ONE ANSWER ONLY)

Very important	1
Fairly important	2
Not very important	3
Not at all important	4
DK	5

QB33 EU data protection rules nowadays provide for special protection for the processing of sensitive personal data, such as data related to health, sex life, ethnic origin, religious beliefs, political opinions, etc. Do you think that genetic information such as DNA data should also have the same special protection?

(READ OUT – ONE ANSWER ONLY)

Yes, definitely	1
Yes, to some extent	2
No, not really	3
No, definitely not	4
DK	5

QB34 Please tell me whether you totally agree, tend to agree, tend to disagree or totally disagree with the following statements regarding the protection of personal data of minors.
(SHOW CARD WITH SCALE – ONE ANSWER PER LINE)

	(READ OUT)	Totally agree	Tend to agree	Tend to disagree	Totally disagree	DK
1	Minors should be specially protected from the collection and disclosure of personal data	1	2	3	4	5
2	Minors should be warned of the consequences of collecting and disclosing personal data	1	2	3	4	5

QB35 The police sometimes access and analyse individuals' personal data to carry out their activities. In what circumstances should the police be able to access individuals' personal data?
(READ OUT – ONE ANSWER ONLY)

For all general crime prevention activities	1
Only specific data within the framework of a specific investigation	2
Only with the authorisation of a judge	3
Never (SPONTANEOUS)	4
DK	5

QB36 Do you think that your data would be better protected in large companies if they were obliged to have a specific contact person in charge of ensuring that your personal data is handled properly?
(READ OUT – ONE ANSWER ONLY)

Yes, definitely	1
Yes, to some extent	2
No, not really	3
No, definitely not	4
DK	5

QB37 In your opinion, the enforcement of the rules on personal data protection should be dealt with at…?
(READ OUT – ONE ANSWER ONLY)

European level	1
National level	2
Regional or local level	3
DK	4

QB38 Have you heard about a public authority in (OUR COUNTRY) responsible for protecting your rights regarding your personal data?

Yes	1
No	2
DK	3

QB39 Some companies use people's personal data without them being aware, creating inconvenience ranging from spam to financial loss. What should be the public authorities' main priorities to fight these practises?

(SHOW CARD – READ OUT – ROTATE – MAX. 4 ANSWERS)

Impose a fine to these companies	1,
Provide legal support for those willing to take the case in court	2,
Provide an out of court procedure to sort out the problem	3,
Ban them from using such data in the future	4,
Compel them to compensate the victims	5,
Put people in similar situation in touch to start joint legal action	6,
Give people more direct control on their own personal data	7,
Allocate more resources to monitoring and enforcing existing regulations	8,
Find better technical solution that preserve users' privacy and safety	9,
Provide formal education and guidelines on safe disclosure	10,
Raise awareness of the implications of unsafe disclosure	11,
Make greater use of warnings and signs to signal possible unsafe disclosure	12,
Other (SPONTANEOUS)	13,
DK	14,

LF-NA-25295-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.

Publications Office

ISBN 978-92-79-23914-4

European Commission
EUR 25295 – Joint Research Centre – Institute for Prospective Technological Studies

Title: Pan-European Survey of Practices, Attitudes and Policy Preferences as regards Personal Identity Data Management

Authors: Wainer Lusoli, Margherita Bacigalupo, Francisco Lupiañez, Norberto Andrade, Shara Monteleone, Ioannis Maghiros

Luxembourg: Publications Office of the European Union

2012 – 176 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-23914-4

doi:10.2791/81962

Abstract

This Report presents the results of the largest survey ever conducted in Europe and elsewhere about people's behaviours, attitudes and regulatory preferences concerning data protection, privacy and electronic identity, both on the Internet and otherwise in their daily lives. It finds that personal data disclosure is increasingly prevalent in the European society, largely due to the expansion of the Information Society. In turn, most services provided in the digital economy rest on the assumption that this data and associated electronic identities are collected used and disposed of according to existing legislation.

The survey shows very clearly how Digital Europe is shaping up. About two thirds of EU27 citizens use the Internet frequently, more than one third uses Social Networking Sites (SNS) to keep in touch with friends and business partners and almost 4 out of 10 shop online. In both of these contexts, people disclose vast amounts of personal information, and also manage a large and growing number of electronic identities.

However, there are equally significant differences among Member States and considerable digital exclusion, mainly due to socio-demographic differences in affluence, education and age.

These are some of the insights of the Eurobarometer Survey on Data Protection and Electronic Identity conducted in December 2010. The results were published in June 2011.

The report builds on the top line results presented in the EB-359 report and analyses in depth the information collected so as to draw conclusions in direct relation to four key Digital Agenda areas: e-Commerce, Social Networking Sites, Authentication and Identification and Medical Information as Personal Data.