Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks

Wainer Lusoli, Caroline Lancelot Miltgen

JRC Scientific and Technical Reports

Young People and Emerging Digital Services
An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks

Authors: Wainer Lusoli and Caroline Miltgen
Editors: Wainer Lusoli, Ramón Compañó and Ioannis Maghiros

EUR 23765 EN - 2009

JRC EUROPEAN COMISSION

ipts Institute for Prospective Technological Studies

Young People and Emerging Digital Services

An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks

Authors:

Wainer Lusoli and Caroline Miltgen

Editors:

Wainer Lusoli, Ramón Compañó and Ioannis Maghiros

2009

EUR 23765 EN

The mission of the JRC-IPTS is to provide customer-driven support to the EU policy-making process by developing science-based responses to policy challenges that have both a socio-economic as well as a scientific/technological dimension.

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

JRC 50089

EUR 23765 EN
ISBN 978-92-79-11330-7
ISSN 1018-5593
DOI 10.2791/68925

Luxembourg: Office for Official Publications of the European Communities

Acknowledgments

This report is based on a study which was conducted with the support of the Lisbon strategy and the i2010 Unit at the Directorate General Information Society and Media. The authors thank Anne Troye and Claire Sion for their guidance during the study, and Michal Hrbaty and Federico Poggi for their review of the report.

The authors would also like to thank Christine Balagué (University of Lille) for her overall contribution to the eID study and for data collection and analysis conducted for this document. She was scientific co-Director of the eID study.

For their assistance at different stages of the project, we are grateful to Margherita Bacigalupo (IPTS), Claudia Cevenini (University of Bologna), Claudio Feijoó (IPTS) and Pawel Rotter (AGH-University of Science and Technology, Kraków and formerly at the IPTS).

Also, we owe a debt of gratitude to the experts who gave their time and shared their knowledge with us during the Expert Workshop held in April 2008.

Finally, we are grateful to Patricia Farrer for her valuable assistance in making the report fully understandable by a larger audience.

Table of contents

List of Tables

Executive summary

This study, conducted by the Institute for Prospective Technological Studies (IPTS[1]), presents the results of a four-country survey of young Europeans' attitudes to electronic identity (eID) and future eID-enabled services. The study aims to remedy the almost complete lack of EU evidence on eID services perceptions. It is innovative in many respects:

- It focuses on young people [15-25], rather than children or adults;
- It targets multiple EU countries [France, Germany, Spain, UK];
- It works with four large national samples [total number of respondents = 5,265];
- It examines eID service scenarios [4 scenarios];
- It retrieves data relevant to policy making.

Based on the opinions of more than five thousand young Europeans, the study demonstrates what aspects of eID and eID services can be measured via a large-scale survey – among them take up, trust, privacy, responsibility, and data control.

Firstly, the survey results give a quantitative measure of young Europeans' perceptions and acceptance of risks, general motivations, attitudes and behaviours concerning eID-enabled services.

1. There are high perceptions of risks, both general and contextual. Most young people are sceptical of the internet as an environment for the exchange of personal data and have major doubts about personal data protection. They perceive high risks in giving personal data and fear that these will be misused in specific eService settings. Additionally, young people see risks to personal data and identity as continuum that spans from the virtual to the real world. Risk greatly hampers the take up of eID services.

2. Young EU citizens are Web2.0 experts and this matters for the future take up of advanced eID-based services. E-mail, search engines and instant messaging are ubiquitous today, and half the respondents also engage in Web 2.0 activities (e.g. sharing pictures) and social networking sites. Young, innovative people, who have been online several times a day for more than 5 years, connecting via broadband, are the digital leaders in relation to eID.

3. Digital culture and markets matter. There are significant differences between countries in terms of digital culture and markets. Spain presents lower social network usage; France has a blogging culture; and youngsters are more skilled in Germany than elsewhere. Computers still rule, PC access to the internet is still prevalent while mobile, using GPRS or 3G, is only used by one in six. Even fewer connect to the internet through gaming consoles. All these factors are important for personal innovativeness, and, in turn, for the take up of eID services.

1 IPTS is one of the 7 research institutes that make up the European Commission's Joint Research Centre

4. eID technologies are perceived differently. PINs and passwords constitute a 'pass partout', biometrics are relatively well understood, IP is on the radar, while RFID and electronic signatures baffle young users. Scenario analysis yields a more positive perception of biometry versus the three other eID systems. Even if familiarity were to be harnessed to increase eID acceptance, the context of service take up matters much more than technologies and general attitudes to personal data protection.

5. There are multiple eID enablers. To encourage the use of eID systems, the key success factors include precise information on eID systems and guarantees, and the enforcement of data protection law. This may be accomplished through: 1) compliance with data protection and privacy principles (revision or new regulations adapted to specific user needs and requirements); 2) good communication (more specifically on the benefits that new technologies can offer) and 3) usability (allowing the user to easily cope with a system's interface).

6. Trust is in the rules of the 'data protection game'. Trust did not emerge in this study as one of the major drivers of adoption, contrary to a wealth of previous evidence. However, young people are demanding procedural fairness in the management of their data. Trust in rules (fair play by eID service providers) is thus an important factor to monitor, in addition to traditional constructs (institution-based, interpersonal, systemic, contextual).

7. Distributed responsibility. Friends and family are more trusted than institutions in relation to the management of personal identity data. Young people do not attribute responsibility for the protection of personal data to governments or police / courts. Instead, they are asking for tools that give them more direct control of their own identity data. Overall, institutions ought to provide a safe, risk-free playing field.

8. A call for 'hands-on' regulation. Young people desire reassurance, via practical tools more than via awareness raising. A first category of tools (guarantees, such as labels and logos) would encourage people to adopt new eID systems. A second set of tools would assist user control of personal data provided to public or private authorities. The call for guarantees is stronger than the call for more personal data control mechanisms.

9. Data protection legislation is unknown and unloved. Young EU citizens' knowledge level about data protection laws is very low. Even lower is their appreciation of the current protection framework. Paradoxically, more knowledge seems not to breed more positive attitudes. Experience may matter more than understanding of the legal system and word of mouth.

10. Gender matters. Female users are more reluctant to use eID technologies than males. This female scepticism may be explained that the female respondents seemed to know less about eID technologies, perceived the risks to be higher and were less willing to disclose data. Gender-friendly eID technologies need to be examined.

Secondly, the study provides tools for evidence-based policy making in relation to eID services. If taken at face value, the results may be used to sharpen policy lines in relation to the regulation (promotion, control) of future eServices. Based on preliminary results from the online survey, we sketch a few practical policy recommendations for the future Information Society that may increase

future take up. These recommendations are necessarily tentative, pending implementation of a wider, more representative survey.

11. Tweak, don't twist. Harness young people's current practices. eID systems must be inspired by personal data management procedures used in social networking sites. Such eID systems may thus be used for a secure log on, allowing youngsters to benefit from a better service, particularly in public utility services. A service to connect with others and valuable information should be linked to secure and safe personal data provision. Further investigation is required into motivations to use value-added services, which can improve daily life and make it easier, at a minimum cost.

12. Look at the wider eID picture, not only eID services. A complex equation involving internet skills, self efficacy, privacy perception, global risks and disclosure needs to be constructed in relation to the efficacy of different regulatory alternatives in relation to eID. Liaise with other important stakeholders in the eID field.

13. Harness eID enablers. Young users place great value on privacy, data control, and free services, but not at the expense of security. The traditional security / privacy paradigm may therefore need revising to include a wider variety of parameters. Guarantees, assurances that data protection law will be protected, and precise information, all of which should encourage the use of eID systems, should be promoted.

14. Reinforce safety concerning privacy and personal data online through technical improvements of eID systems. In parallel to technical improvements, investigation of usage patterns regarding eID systems would contribute to an understanding of the perceptions of eID systems and ways to enhance the take up.

1. eID survey rationale

This report presents the results of quantitative research exploring EU young people's behaviours and attitudes towards electronic identification system (eID) and eID-enabled services in particular. eID is 'a system adopted by an organization (business or government) for the issuance and maintenance of electronic identities of individuals'. eID-enabled services include currently available services (connecting to friends via mobile phone SIM card, Social networking sites such as Facebook, Skype, online banking and online grocery shopping) and more advanced services (RFID tags may advise people on purchases as they walk past; travel agents may suggest additional sightseeing based on customer GPS position; biometric, e.g. eye-scanning may be used to access physical areas); all these services, present and future, require the ability for the user to be identified, authenticated, and, in many cases, profiled.

Hence eID transactions raise crucial issues in relation to trust, privacy, data control, transparency, awareness, all of which affect the fruition (and the supply) of eID enabled advanced services. The main aim of the survey is to investigate the way people take the decision to adopt (or not) a new service including electronic identification means. This sheds light on the future adoption of eID-based service and on the barriers, enablers and circumstances of such adoption. The survey aims to identify key factors supporting the development of actual and potential eID systems, in the views of young European consumers.

The report is part of a larger study examining eID systems adoption and perceptions in Europe. The study devised and tested a methodology for the large-scale survey of needs and requirements on future eID and the barriers and enablers of eID-based services, specifically for young people; to understand the desired shape of eServices to come and what matters for fruition, and whether the public is ready (or not) to adopt eID services; and to propose sound, reliable benchmarks for the monitoring of trends in the demand for eID and eID-enabled services in the near future.

The study comprises desk research, focus groups in four countries, an expert workshop, a survey pre-test and an online survey conducted in four countries and involving more than 5,000 young people. Overall, the study was intended as a dry-run to test the feasibility of a pan European survey regarding young people's attitudes to eID services. This is not discussed specifically in this report.

A first questionnaire was proposed by the team and discussed by experts (law, ICTs, marketing) at a validation workshop in April 2008. The workshop helped to modify the research framework and to improve the questionnaire. The revised questionnaire was tested with 117 young people in the UK at the end of June 2008. Results of the pre-test were used to streamline the survey and reformulate some questions. The pilot also gave first figures on email return and open rates and helped to optimize the number of sent emails in order to get sufficient (statistically) answers for data analysis. The final questionnaire (Appendix 1) was sent to more than half a million young people ages 15 to 25 in France, UK, Spain and Germany, exploring perceptions, attitudes towards and intent to adopt eID services. It obtained 5,265 full responses and about 6,000 additional partly completed responses. This report presents main findings from the research process and the results of the survey.

The report is organized as follows:

- This section provides a brief overview of the study's context. We outline the survey's scope and main objectives in the economy of the study. We present the theoretical framework regarding eID and advanced e-services on which the questionnaire is based.
- Section 2 focuses on survey methodology. We explain the method chosen to administer the questionnaire and detail the sample. We discuss the challenges encountered during implementation. We discuss data analysis and the validity of the results.
- Section 3 reports the survey results. We provide top line results and present more complex analysis (multivariate, modelling). Inter-country comparative results and scenario results are given along with some conclusions.
- In Section 4, we offer a discussion of the results and propose recommendations and lessons for a prospective pan-European survey.

1.1. Main results from the literature review

Very limited survey data exist on public perceptions of eID systems in the EU, especially in relation to young people. Also, the concepts studied in existing surveys have not always been measured with the same items. Consequently, it is difficult to compare directly our results with similar previous topics. There are six exceptions to this.

- Eurobarometer Flash for DG INFSO[2] – EU27 study on confidence in the Information Society, with questions on security risk awareness / knowledge, damage and protective behaviours.
- Eurobarometer Flash for DG JLS[3] – EU27 study, with questions in relation to data protection overall in own country, plus one on privacy-enhancing technologies and one on internet trust.
- OCLC report[4] – a comprehensive survey, although limited to privacy, trust and only three EU countries.
- OECD report[5] – review of safety and security official statistics focussing mainly on security, with limited if no focus on identity.
- FIDIS Survey[6] – 19-country web survey limited to perceptions of institution-based trust in the handling of personal data.
- EU Kids Online project[7] – repository of survey and other evidence in relation to online safety and risks of children and adolescents.

Whereas responding to the challenges to privacy and trust stemming from new converging services in the future ubiquitous information society is flagged as a recommended action in the i2010 - Mid-term review,[8] there seem to be no plans for measuring any of the relevant constructs using official EU statistics, even after

2 Gallup, Confidence in Information Society. (Brussels: EC DG INFSO, 2009). <forthcoming>.

3 Gallup, Data Protection in the European Union - Citizens' Perceptions (Brussels: EC DG JLS, 2008). Available from <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>.

4 Rosa, C. D., et al. Sharing, Privacy and Trust in Our Networked World. Dublin, OH: Online Computer Library Center, 2008. Available from <http://www.oclc.org/reports/pdfs/sharing.pdf>.

5 M. Schaaper, Measuring security and trust in the online environment: a view using official data (Paris: EAS, DSTI, OECD, 2008). Available from <http://www.oecd.org/dataoecd/47/18/40009578.pdf>.

6 Backhouse, J., and R. Halperin. "A Survey on Citizen's Trust in Id Systems and Authorities." Fidis Journal 1.Online (2007). Available from <http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf>.

7 See http://www.eukidsonline.net/

8 European Commission, Communication from the Commission - Preparing Europe's digital future i2010 - Mid-term review (Brussels: European Commission 2008). Available from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0199:EN:HTML>.

recent revision of the Regulation on Community statistics on the information society.[9]

Due to the lack of systematic survey evidence, the study reviewed a significant number of research studies on ICT in general and in particular on the topics of identity, identification, personal data sensitivity, security and privacy. It reviewed technological and regulatory trends and challenges in ICT and eID systems and analyzed these trends from a user perspective in order to identify the main needs and requirements of European citizens towards eID. Here are the main points from the review, useful to contextualise the survey.

1. Contradictory perceptions on ICT and eID systems exist. While such technologies are not always seen as dangerous or risky, EU citizens demand more security and privacy, personalization of services, ease of use and better content quality. The survey thus evaluates the public perceived benefits and risks towards eID systems in order to evaluate their intention to adopt such systems.

2. People are concerned about threats to privacy when using online services but are not concerned about the amount of information available on them online (the so-called privacy paradox). Consumers routinely declare that they value their privacy highly but do not seem to actively incorporate privacy concerns in their transactions. More generally, the public is primarily concerned about losses of privacy that lead to security problems but few everyday activities are considered extremely or very private. Identity theft is among the top privacy concerns in public opinion. While having controls and rules on how personal information will be used is very important to citizens, people use real names when registering on websites. The ability to remain anonymous and to specify who can view and use their information are important to people, but they do not frequently use these controls. The survey evaluates the importance and the causes of this 'privacy paradox'.

3. Online identity matters. People and young people in particular use real name and provide personal identity data such as address and demographics when registering on websites. However, people expect control and rules on the use of their personal data - i.e. control over who uses this data and to what extent. Privacy policies, codes of conduct and security icons are important to people but they do not frequently use these controls on social networking sites. Nether they carry themselves online in a way conducive to minimum disclosure, with minimum time taking care of their 'digital persona' (an identity paradox?). In the survey, we explore how young people consider their identity and manage personal data online.

4. Many citizens are unaware of their rights and feel unable to know what actually happens to their data. Consequently, they do not trust institutions' competence to handle personal data. Moreover, citizens live in a culture of distrust and suspicion which hampers implementation of eID scheme in Europe. Therefore, the survey explores the level of knowledge and use of and trust in regulatory and other data protection means, and people's perceptions of regulation.

5. A successful deployment strategy for new eID systems requires that privacy interests

9 European Commission, "Commission Regulation (EC) No 960/2008 of 30 September 2008 implementing Regulation (EC) No 808/2004 of the European Parliament and of the Council concerning Community statistics on the information society Text with EEA relevance," Official Journal L 262.01/10/2008 (2008). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:262:0006:0022:EN:PDF. The only forthcoming item fitting with the topics addressed in this study is [(optional) awareness of fundamental rights of consumers in the EU in connection with online purchases of goods over the internet (except auctions): privacy and data protection].

are balanced with the benefits that advanced services may offer. The survey need to investigate the extent to which people are aware of new identification means and perceive their costs (risks, privacy and confidentiality) and benefits.

6. Trust is key success factor for the implementation and acceptance of new ICT and eID applications. Building trust in the citizen and end-user could be a key success factor for the eID innovation to be adopted. Trust will be examined in the survey.

7. Existing studies show that the majority of the population is unaware of the risks posed by the collection and use of personal information and technologies that should help them in protecting their privacy. This level of awareness should be moderated by existing differences between member states, as attitudes and behaviours towards the implementation of new eID systems may differ from one country to another. The survey evaluates the level of public awareness in different countries.

The findings are further articulated in Section 1.3, which presents the theoretical framework of the survey.

1.2. Focus groups results

Focus groups with 15-25 years old Europeans in four countries were conducted before the survey. Focus groups aim to avoid elaborating a questionnaire based on elements chosen only by researchers. The main objective was to allow youngsters to express themselves on these topics and to let them talk about their motivations or reluctance to adopt such new electronic applications as well as their perception of the risks. We aimed to investigate what young Europeans think about issues of identity, protection of personal data, security, privacy and eID systems. Discussions addressed the issues of perceived, acceptance levels of risks, general motivation, intent to adopt and specific needs for ICT in general and especially eID technologies.

Two focus groups of eight to 12 participants were held during January and February 2008 in Spain, France, Germany and the UK. Focus groups ran for approximately one and a half hours and were conducted by a qualified researcher specialized in qualitative research and/or in one of the topics studied (i.e. ICT, privacy). Participants were asked for their views of the perceived advantages and disadvantages of new technologies (especially the Internet) and for their understanding of issues of security and privacy. They were also asked about electronic identification systems (risks, motivations to adopt and intent to use) and regulatory issues. Groups were audio and video recorded, transcribed and then analyzed to capture key points, positions and opinions.

The results of the focus groups confirmed findings from previous studies and highlighted some differences. The discussion groups confirmed the importance of risk. Young European people mainly evoked security and privacy issues and confirmed that they fear unauthorized use of personal data. They asked for more controls on data use, more particularly who uses their data and to what extent. Identity theft was mentioned in relation to online commerce and online banking. Results also confirmed the so-called privacy paradox: consumers at the same time declare that they value they privacy and do not seem to actively incorporate privacy concerns in their behaviour.

Results confirmed that a large majority of young European are sceptical concerning the implementation of eID systems. Youngsters are generally unaware of existing eID systems and doubt the capability of public organizations to manage these systems and offer real protection against security and privacy breaches. Some

elements facilitate the use of eID applications: familiarity with the systems, attribution of labels providing guarantees to the users, trust, knowledge of eID systems and of specific regulatory issues. However, results confirmed that today the young European people are quite unaware of existing laws on data protection and related rights.

Other results provided details on how youngsters define identity and how they manage it online. For example, they make a clear distinction between identity and personal data: identity refers to sensitive information, personal data are mostly considered as public data accessible to everyone. Finally, results complemented existing literature concerning member states specificities. For instance, German and French youth have a different level of knowledge concerning eID systems. There is a gap concerning the feelings about the ability of public organizations to manage them (different in Spain and in Germany) and the need for repressive laws. These results suggest an adoption process and reactions to eID implementation very specific by country on certain aspects.

1.3. Theoretical framework

A first, long version of the survey questionnaire was discussed in an expert workshop held at the IPTS during April 2008. This included a significant degree of redundancy. On the basis of experts' recommendations, a questionnaire was revised that was 21 questions shorter than the original and significantly leaner. The revised questionnaire is enclosed as Appendix 1.

In this section we discuss the theory relevant to questions and sections included in the final survey; we discuss the value of single questions when presenting the results, and propose further amendments to the questionnaire in the conclusions.

The main theories which served as a basis to our conceptual framework in order to measure European people's perceptions in relation to adoption of eID services were:

1. Individuals' perceptions of technology (based on the Technology Acceptance Model),
2. Adoption characteristics (based on Diffusion of Innovation Theory),
3. Individuals' perceptions of risks and negative consequences,
4. Trustworthiness of organization, eID technology and Internet,
5. Other predictors cognate to the Technology Acceptance Model.

The starting point of the discussion here is that we aim to measure intention to use advanced eID services, which for the most part do not exist or are in early phases of implementation, where access would be impractical. Therefore, we set the research focus for the survey on intention to use, rather than on use of such services. Attitudes and behavioural intentions have been shown to be reliable predictors of behaviour across a wide range of domains and provide efficient means of assessing behavioural outcomes. Measuring intention to adopt a new technology (e.g. an eID application) can thus be seen as an effective way to evaluate the potential successfulness of the innovation. That is why we measure the intention to adopt the technology (i.e. the eID system) as a key dependent variable of our conceptual framework. Attitude toward using the proposed eID scenario had also been included in the questionnaire as well as the intent to recommend it to friends.

According to the technology acceptance model (TAM), perceived usefulness and perceived ease of use (PEOU) influence one's attitude towards a technological system, which in turn influence one's behavioural use intention. PU is 'the degree to which a person believes that using a particular system would enhance his or her job performance', and PEOU as 'the degree to which a person believes

that using a particular system would be free of effort'.[10] Moreover, perceived ease of use is believed to influence perceived usefulness, the easier a system is to use the more useful it can be. These constructs reflect users' subjective assessments of a system, which may or may not be representative of objective reality. These two constructs have already been used in studying the intent to adopt ICT and/or specific eID systems, large and small, such as the intent to adopt new software in four industries[11] or electronic toll collection service adoption.[12] Perceived usefulness and perceived ease of use have thus been included in our conceptual model.

According to the Diffusion of Innovation Theory, the rate of technology diffusion is affected by an innovation's relative advantage, compatibility, trialability, observability and complexity. Research suggests all but the last factors have a positive influence on diffusion. Relative advantage is 'the degree to which an innovation is seen as being superior to its predecessor'. Complexity, which is comparable to TAM's perceived ease of use construct, is 'the degree to which an innovation is seen by the potential adopter as being relatively difficult to use and understand'. Compatibility refers to 'the degree to which an innovation is seen to be compatible with existing values, beliefs, experiences and needs of adopters'. Trialability is the 'degree to which an idea can be experimented with on a limited basis'. Finally, observability is the 'degree to which the results of an innovation are visible'. Overall, relative advantage, compatibility and complexity are most relevant to adoption research. Moreover, complexity is comparable to TAM's perceived ease of use construct, while perceived usefulness and relative advantage are, according to many, the same construct. In the study we opt for the well-tested TAM constructs rather than for similar DOI constructs. In addition the discussion during the workshop concluded that these DOI constructs were not necessarily adapted to our model as the eID systems that we wanted to test didn't exit at the moment. The constructs of trialability and observability were consequently impossible to measure. As a result, our conceptual framework will only include compatibility as a DOI construct.

In addition, as one of the main research lines in relation to eID involved the perceived dichotomy between convenience and security (that is, users behaving less than securely to avail from free services) perceived benefits such as economic gain, time saving and overall convenience were included These indicators were found to be strong predictors in the adoption of telephone and cable services.[13] All the more, economic benefits could affect the adoption of eID systems and are thus included in our model.

It is well known that these constructs focus on key factors to innovation adoption relate, mainly gauging perceived advantages of a technology. However, the study also takes into account various obstacles to adoption. Most studies on personal information disclosure show that consumers' reluctance to disclose information that is personally identifying is theoretically attributable to corresponding differences in the perceived severity of negative consequences (risks) of disclosure. But, only expectations of negative consequences of complying with the demands of a specific innovation and not generalized risks should be considered. The perceived risks are linked to particular decisions (for example, the decision to self disclose or not) which can occur in specific

10 F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS quarterly 13 (1989).

11 V. Venkatesh, M. G. Morris, G. B. Davis and F. D. Davis, "User acceptance of information technology: toward a unified view," MIS quarterly 27.3 (2003).

12 C.-D. Chen, Y.-W. Fan and C.-K. Farn, "Investigating Factors Affecting the Adoption of Electronic Toll Collection: A Transaction Cost Economics Perspective," Proceedings of the 40th Annual Hawaii International Conference on System Sciences (IEEE Computer Society, 2007).

13 R. LaRose and M. S. Eastin, "A Social Cognitive Theory of Internet Uses and Gratifications: Toward a New Model of Media Attendance," Journal of Broadcasting and Electronic Media 48 (2004).

circumstances and time (task, context and time specific). Consequently, as with all innovative technologies, specific risks linked to the adoption of this technology should be measured in order to address the specific perceptions of people. For example the adoption of new monetary device includes financial risks which are not so important when considering the adoption of electronic administration. The framework therefore gauges perceived risks relative to eID applications. For eID, financial, safety and psychological risks are most often discussed. For example, financial risks include third party accessing to personal details of users (e.g. credit card). It has been shown that perceived risk is associated with lower consumers' intentions to use Internet sites for transactions.[14] In our study, it is expected that perceived risks would lower consumers' intentions to adopt a new eID application.

A further construct relevant to eID relates to trust, and more specifically to perceived trustworthiness. There is theoretical and empirical support for integrating trust in DOI and TAM. Many studies of eGovernment services suggest that perceived trustworthiness could impact citizens' intention to use. Trustworthiness is 'the perception of confidence in the electronic marketer's reliability and integrity'.[15] A multidimensional model of trust in e-commerce focuses on users' initial trust in a web vendor.[16] Institution-based trust is associated with an individual's perceptions of the institutional environment, such as the structures, regulations and legislation that make an environment feel safe and trustworthy. This construct has two dimensions: structural assurance and situational normality. Structural assurance means 'one believes that structures like guarantees, regulations, promises, legal recourse or other procedures are in place to promote success'. Situational normality presumes that the environment is normal, favourable, in proper order and that vendors have competence, benevolence and integrity. Most work on e-commerce includes benevolence, integrity and competence as key concepts to evaluate institution-based trust. Following the theory of reasoned action, trust creates positive attitudes toward organizations that are likely to reduce fears of opportunism and attenuate infrastructure concerns, in turn influencing positive consumer attitudes which have an effect on behavioural intentions to adopt new technologies, for instance by the influence of trust on the intent to shop online. For instance, perceived trustworthiness significantly influences the intention to use e-government services.[17]

But citizens must have confidence both in the providers and in the enabling technologies. Trust models suggest that a combination of trust in the internet, in the merchant (or organization trying to implement the innovation) and in the product or service proposed (here: eID) affects overall perceptions of trustworthiness.[18] The decision to adopt new eID systems requires citizen trust in the organization providing the service and in the technology through which electronic transactions will be executed (e.g. payment in the context of electronic payment or identification for new eID systems). These components should be evaluated individually and in combination, within the context of new eID systems' implementation. As the Internet is the main platform on which eID system are implemented and available, trust in Internet should be measured. We include three additional constructs in our conceptual framework: trust in the organization implementing

14 A. D. Miyazaki and A. Fernandez, "Consumer Perceptions of Privacy and Security Risks for Online Shopping," Journal of Consumer Affairs 35.1 (2001).

15 Belanger, F., J. S. Hiller, and W. J. Smith. "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes." Journal of Strategic Information Systems 11.3-4 (2002): 245-70.

16 McKnight, D. H., V. Choudhury, and C. Kacmar. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology." Information Systems Research 13.3 (2002): 334-59.

17 L. Carter and F. Belanger, "The utilization of e-government services: citizen trust, innovation and acceptance factors," Information Systems Journal 15.1 (2005).

18 Lee, M. K. O., and E. Turban. "A Trust Model for Consumer Internet Shopping." International Journal of Electronic Commerce 6 (2001): 75-92.

the system, trust in the enabling technologies and trust in Internet.

To improve the viability of TAM in information system research an in information systems adoption it was recommended to incorporate 'external variables'.[19] We include in the survey individual independent variables and situational variables. Social identification theory argue that three factors have a conjoint influence on self-identification: the actor, the audience (person or organization with which he is dealing) and the situation. Elements linked with the actor himself are included in the individual variables presented above. Elements concerning the audience refer to the person or the organization with which the actor is dealing. Consequently, we have included questions on the organizations people trust more in collecting and using their personal data.

Finally, eID practical applications may influence public perceptions. For example, whether the system includes or not biometric recognition may engender different public perceptions. In order to assess different types of eID system, we put respondents in a simulated situation where eID applications were described in a written scenario. Four scenarios concerning eID applications (e.g. biometrics, mobile, etc) were eventually tested.

Individual-level variables

Individual-level variables included in the questionnaire belong to four categories.

1. Demographics

Analysis of most surveys' results points to the role of demographic characteristics in influencing people's perceptions towards ICT. For example, in a survey on EU Citizens' trust in ID systems and authorities, Backhouse and Halperin found that gender features strongly in citizens' perception of trust: in general, male respondents were more negative in their views. In the questions about the legal framework, the difference was 20 percent between the number of 'strongly disagree' answers for the groups of women and men respectively. Age has also a strong influence: younger people tended to exhibit more openness towards eID cards than older respondents. As a result, the following demographic variables were measured in the questionnaire: country of origin/ nationality, age, gender, settlement size (rural/ urban), education level, occupation, parents' occupation.

2. Psychological and personality variables

Because of novelty, adopting an innovation such a new IT or eID system inherently involve a risk. Some people are more or less likely to take a risk in adopting an innovation due to their differences in innovativeness. That's why we propose to introduce the fear of technology or, better, its opposite, the person's innovativeness in our questionnaire. DOI define innovativeness as 'the degree to which an individual or other unit of adoption is relatively earlier in adopting new ideas than other members of a social system'. Researchers utilize three mechanisms to classify innovation adopters into adoption categories: the innovativeness construct, a set of consumer behaviours, and 'years to adopt'. The use of the former is deemed a more precise approach. A metric was advanced for the measurement of domain-specific individual innovativeness, focusing on the adoption of IT and a scale named 'personal innovativeness in the domain of IT', defined as 'the willingness of an individual to try out any new information technology'.[20] Because this scale is specific to IT systems, it seems particularly adapted to our study.

19 Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology."

20 Agarwal, R., and J. Prasad. "A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology." Information Systems Research 9.2 (1998): 204-15.

3. 'Experiential' variables

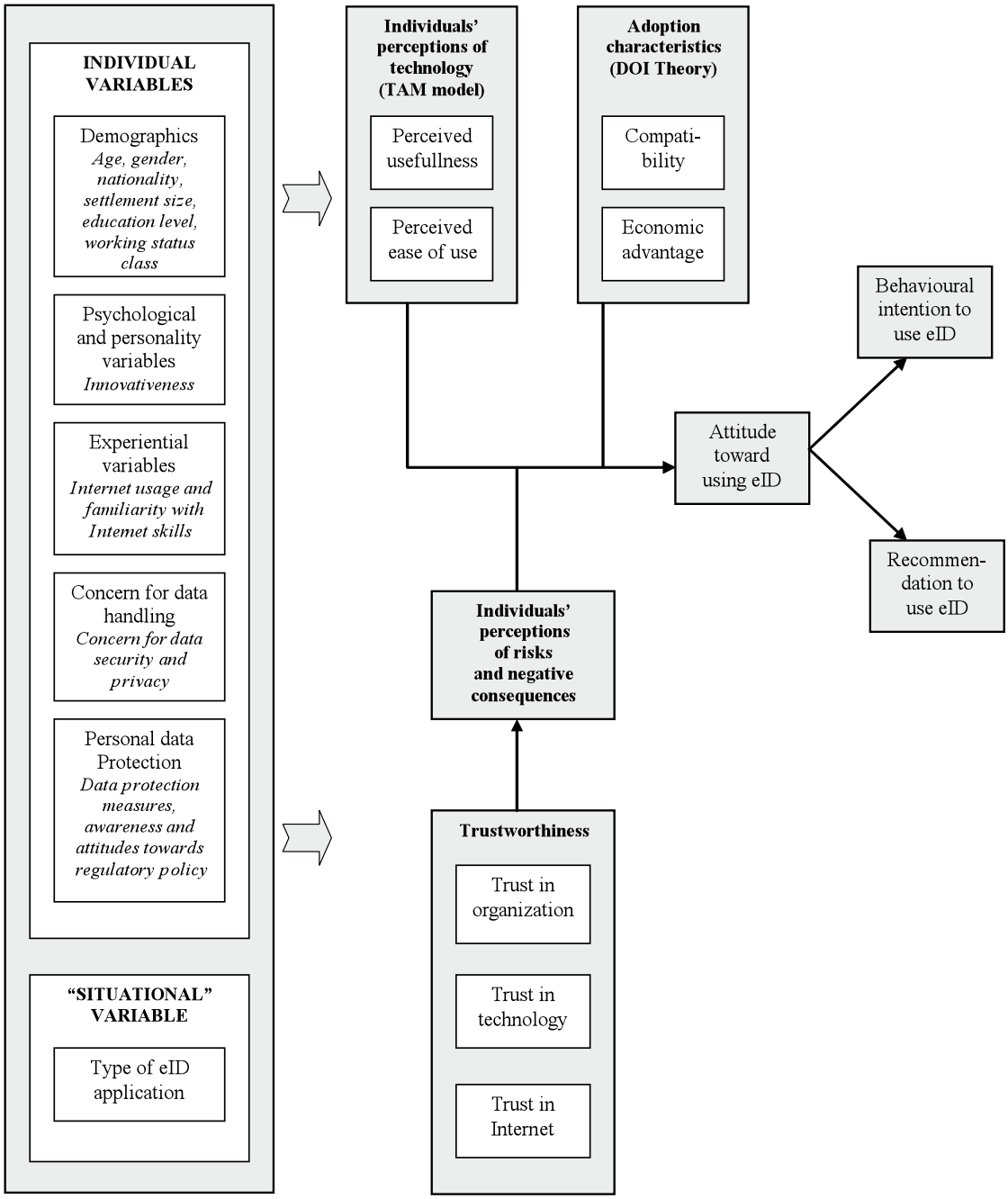
We considered as 'experiential' variables the factors which should be linked with the experience the individual has with the technology in general, Internet and Privacy intrusion in particular. Extensive use of the Internet tends to lower perceptions of strong disagreement.[21] Consequently, several variables related to Internet usage will also be measured in the survey questionnaire. The variables on Internet usage and familiarity which have been measured in the survey included: Internet length of use, connexion frequency, place of connexion, connexion devices and Internet skills.

4. Attitudes and behaviours in terms of personal data handling and protection

We have included in our questionnaires measures concerning: 1) concerns for data handling (including privacy concern) and 2) data protection awareness, attitudes and behaviours. Until now, concern for privacy has been neither defined nor measured consistently. Almost every author has its own definition and measure of this concept. This concept mainly reflects an individual's perceptions of the risks associated with potential privacy violations that may incur during information practices. Moreover, the measures more widespread are also the longer ones. As we cannot use as many items for a single concept, we have tried to find shorter scales that were also mainly used by 'privacy' authors. As data protection is an important public concern, we have also included questions on data protection measures used by people in order to protect their privacy. Moreover, we also measured the awareness and attitudes towards regulatory policy concerning data protection in Europe.

21 Backhouse, J., and R. Halperin. "A Survey on Citizen's Trust in Id Systems and Authorities." Fidis Journal 1.Online (2007). <http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf>.

Table 1 Survey theoretical framework



2. Survey methodology

This chapter outlines survey design and the challenges encountered during its implementation. We present the sample and questions concerning the methodology and the validity of the results.

2.1. Survey design

The initial choice of countries, administration mode (online) and sample size were set in agreement with the client in the early stages of the project and were unchanged throughout. The main objective was to design an online questionnaire to be administered to young people aged 15-25 in 4 European countries (France, UK, Germany and Spain) with a minimum of 1,000 responses in each country. We recommended that the survey be carried out with online auto-administrated questionnaires in large countries where Internet access is widespread. The number of countries was limited by budget constraints.

Online surveys have clear advantages:

- Powerful: Internet allows us to collect and store a significant amount of data.
- Flexible and accurate: questionnaires can be run very quickly, test hypotheses easily and manage different targets.
- Interactive: questions can be adapted based on previous answers, which maximizes the customization of the questionnaire.
- Low cost: much cheaper than offline surveys; this enables to experiment with question format, structure, framing.

Eventually, the survey involved more that 12,000 young Europeans between July and August 2008. Participants in the study were diverse in nationality, gender, age, professional status and education level. The survey aimed to ensure that the methodology and the questionnaire could be expanded to a subsequent larger-scale survey. The results of this survey lead to practical recommendations for the extended large-scale pan-European survey and provide indications about its boundary conditions. Some of these recommendations are not discussed in this report.

The results from this study are 'theoretically generalisable', in that there is no reason to assume that our sample of participants is specifically atypical (e.g. all middle class, or all men) and the analysis is rigorous and systematic (Mason 1996). In this respect, the findings presented here can be taken to indicate current young Europeans' attitudes towards ICT in general and the Internet and identification systems in particular.

2.2. Sampling

The survey was carried out by the French company 1000Mercis.com on behalf of the research team, based on their database Elisa. Elisa is a laboratory to test, analyse and understand Europeans' behaviours and attitudes. Elisa is an opt-in programme sending targeted promotional offers by email, SMS or postal mail. This programme is compliant with European Regulations as well as with its French transposal. This database has nine million members living in Europe and 500,000,000 profiling criteria. 1000Mercis.com partners collect behavioural data through their online activities and rely on 1000Mercis for data housing, data cleaning, data management and rental. This database is multi-cultural, efficient (good response rate) and allows to obtain a representative sample of young European people.

The sample was selected by quotas from the Elisa database. This method was selected because random sampling was unavailable. An email database of young citizens between 15-25 years in France, UK, Spain and Germany which would allow random sampling is not available. Quotas were set for gender (male/female) and age (15-18 vs. 19-25). Quotas were based on EUROSTAT data in the four countries. Table 2 presents EUROSTAT Data for 2008, giving the split of the population on sex and age.

Table 2 Repartition of European population (EUROSTAT 2008)

	France	UK	Spain	Germany
	%	%	%	%
Male	51	51	51	51
Female	49	49	49	49
15-18	36	36	33	35
19-21	28	28	26	28
22-25	36	38	41	37

Based on the response rate achieved in 1000mercis's previous studies, we aimed at targeting 26,042 individuals per country. The objective was to obtain 1,500 respondents per country which makes it possible to achieve a representative sample of 1,000 respondents (15-25 years old) per country. we encountered two main challenges during the implementation of the questionnaire which affected sampling, directly and indirectly. The first one concerns the pre-test. The second one is about translation.

Pre-test

The revised questionnaire was tested with 5,000 young people in the UK at the end of June 2008. The results of this pre-test were used to amend, remove and reformulate some questions. Pre-tests are common in the implementation of large-scale surveys. Generally, they allow anticipating open rates of a questionnaire, looking at the understanding of the questions by respondents, quantifying the time to fill the questionnaire, and finally making adapted corrections in order to optimize the final return rate and number of valid responses to each question. The pre-test was sent to 5,000 young people in the UK. Only 117 people begun to answer the questionnaire and only 20 answered the whole questionnaire (Table 3). These results are low by any standards.

Table 3 Pre-test questionnaire results

Emails sent	5,000	
Opened emails	868	17%
Clicked	164	19%
Completed	20	13%

In brief, pre-test results showed three problems.

1. People did not open the email (17% did, or 1/6)
2. People did not click on the link (19% did, or 1/5)
3. People did not complete the questionnaire (12% did, or 1/8)

There are two reasons for the low open rate. The first is the delay from the initial plans on account of the amendments following the expert workshop and of the translations. Originally planned in early June, the pre-test shifted one month to July, which was a worse time to reach young people who had by then already finished school. Second, the length of the questionnaire, even after reduction at the workshop, was an issue, along with complex scales and labels. To address these problems, the following solutions have been used.

1. To solve the open rate problem:
   - We asked 1000mercis to send email invitations to more respondents than planned. Eventually, 530,000 emails were sent, five times more than agreed

at no additional cost. One advantage of online administration is rapid response to increased emails sent.

- We asked 1000mercis to send reminders to non respondents with different texts according to the stage where they dropped out (no click on the email or drop out before the end). Better open rates were obtained following this action.

2. To solve the click rate problem, we:
   - Included the EU logo (blue field with stars).
   - Revised the text to stress that the survey was very important.
   - Signed the questionnaire, so that the message appeared personalized.

3. To solve the response rate problem, we:
   - Shortened the questionnaire by three questions.
   - Cut response options (items) on three questions.
   - Changed the level of measurement in four questions, to make it quicker to respond.

Overall, the pre-test was useful to evaluate return rates and to amend the questionnaire. Table 4 presents the prediction of the results after the pre test compared with results of the survey, good compared with expectations.

Translation

A second challenge was the translation in three languages (original in English), especially with respect to:

- translation of attitudinal questions as they were country specific,
- translation of socio-demographic items (e.g. education level, occupation),
- translation of invitation e-mail,
- time required to translate the questionnaire,
- specificity of young people 'slang' in relation to internet in different countries.

Eventually, we decided to tailor socio-demographic questions to each country. While this solution is interesting, it somewhat limits the comparison between countries.

Survey administration

After translation, the online survey was sent to 531,443 young people in France, UK, Spain and Germany, in July and August 2008. The process of recruitment is described in Table 5. The survey obtained 12,143 responses to the first question and 5,265 responses to the whole questionnaire. The initial criteria of a minimum of 1,000 respondents was respected in all

Table 4 Comparison of pre-test expectations and survey actual response rates

	Estimated rates after current modifications and accounting for seasonality			
	France	**UK**	**Germany**	**Spain**
Expected unique open rate	20%	15%	15%	20%
Achieved	37%	14%	12%	19%
Expected click rate	22%	18%	18%	20%
Achieved	19%	15%	14%	14%
Expected post click response rate	65%	60%	60%	60%
Achieved	49%	57%	49%	80%
Expected completion rate	30%	30%	30%	30%
Achieved	45%	48%	48%	35%
All expectations were made on July 7, 2008				

Table 5 Survey totals

	France	UK	Germany	Spain	Total
Emails sent	129,828	143,476	101,086	157,053	531,443
Invalid email addresses	1,580	3,000	3,015	559	8,154
Invalid email rate	**1.2%**	**2.1%**	**3%**	**0.4%**	**1.5%**
Valid email addresses	128,248	140,476	98,071	156,494	523,289
Emails opened	47,724	20,209	12,009	30,149	110,091
Open rate	**37%**	**14%**	**12%**	**19%**	**21%**
Emails clicked on	9,155	3,020	2,672	4,240	18,087
Click rate	**7.1%**	**2.1%**	**1.7%**	**2.7%**	**3.5%**
Respondents to the first question	4,485	2,631	1,709	3,318	12,143
Respondents to the last question	2,014	1,258	819	1,174	5,265
Full answer rate	**45%**	**48%**	**48%**	**35%**	**43%**

countries but Germany, where the number of completed questionnaires was n = 819.

As it was noted, 1000mercis agreed to increase at no additional cost the number emails by about 100,000 per country to maximize response rate after the pre-test. An unequal number of emails were sent in each country (e.g. 129,828 in France vs. 101,086 in Germany), partly due to the size of national database. In fact, recruitment was quite different in each country. The French database was very reactive with high open and click rates and low invalid emails rate. This is the opposite in Germany, where the number of invalid email addresses is high and the open and click rates low.

- France: one single mail was sent on 25 July and no reminder.
- UK: a first email was sent to 83,007 people on 25 July with 3 reminders (two specific to 'drop out' respondents) and a second email has been sent to 24,859 youngsters on 13 August (no reminder).
- Germany: one first email was sent to 55,817 people on 28 July with 2 reminders (one specific to 'drop out' respondents) and a second email was sent to 19,638 youngsters on 13 August (no reminder).
- Spain: one single email was sent to 89,119 people on 28 July with 2 reminders (one specific to 'drop out' respondents).

Recruitment management by the contractor when pre-tests gave low results in terms of open and return rates, was crucial. In comparison with the pre-test, the survey obtained better open rates in France and Spain. Survey click rates in France are also better than those of the pre test. However, the final number of full respondents comes principally from the high number of emails sent in each country. This has clear implications for sample representativeness, discussed below.

2.3. Representativeness of the sample

This section describes sample profiles and characteristics of young EU participants. The description covers demographics (Table 6) and data about Internet use (Table 7).

- Of 12,143 respondents, 37% are French, 27% Spanish, 22% UK and 14% German.
- Overall 56% are male and 44% female, this proportion being quite different in some countries, notably in Spain (78% male) and in UK (35% female).

Table 6 Main demographic characteristics of the sample

		France	UK	Spain	Germany	Total
Country responses		37	22	27	14	100
Sex	Male %	60	65	78	53	56
	Female %	40	35	22	47	44
Age	15-18 %	59	30	45	37	46
	19-21 %	31	29	27	29	29
	22-25 %	10	41	28	34	25
Professional status	Student %	56	75	20	54	48
	Self-employed %	1.5	4	9	3	4
	Manager %	1.5	4	3	1	2
	Other white collar %	5	7	6	5	5
	Blue collar %	27	3	51	30	31
	Unemployed %	9	8	11	7	9
Education level	Baccalaureate %	32	62	34	67	39
	Licence %	46	31	37	28	41
	Master %	21	6	22	5	18
	Doctorate %	1	2	8	0	2

- The majority are between 15 and 18 years old (46%), 29% are between 19 and 21 and 26% are 22 years old or older. There are less young people for UK and Germany.
- Nearly 50% are students (more students in UK and less in Spain). Around 30% of young people are 'blue collar' workers (but only 3% in UK and 50% in Spain).
- Considering education, only 2% have a Doctorate and 18% a Master (less in UK and Germany). The most common degree is 'licence' with 41% (only 30% in UK and Germany).

Overall, therefore, there is considerable variance in terms of socio-demographics across the four countries. In future studies, steps need to be taken to standardise the parameter estimates of the sample on those of the population. As with most sampling methods, online and offline, final respondents may not correspond to the initial sample.[22]

In terms of Internet access and use (Table 7):

- Most of the young people in the sample do not have an Internet connection at home (64%) but it does not prevent them from surfing online.
- The majority have used the Internet for more than five years (63% overall and more than 70% in UK) A majority of them surf online several times a day (77% with less people doing so in Spain and more people in France and Germany).

22 To ensure this correspondence, four possible solutions may be proposed: 1) offline administration of the survey, implying a higher cost but higher representativeness; 2) in the context of an online survey, sending additional targeted emails until each quota is filled (implies additional costs); 3) making a random sample on non respondents and elicit answers to verify if their answers differ from those of first respondents; and 4) weights can be attributed respondents to make them representative of the global population.

Table 7 Internet use characteristics of the sample

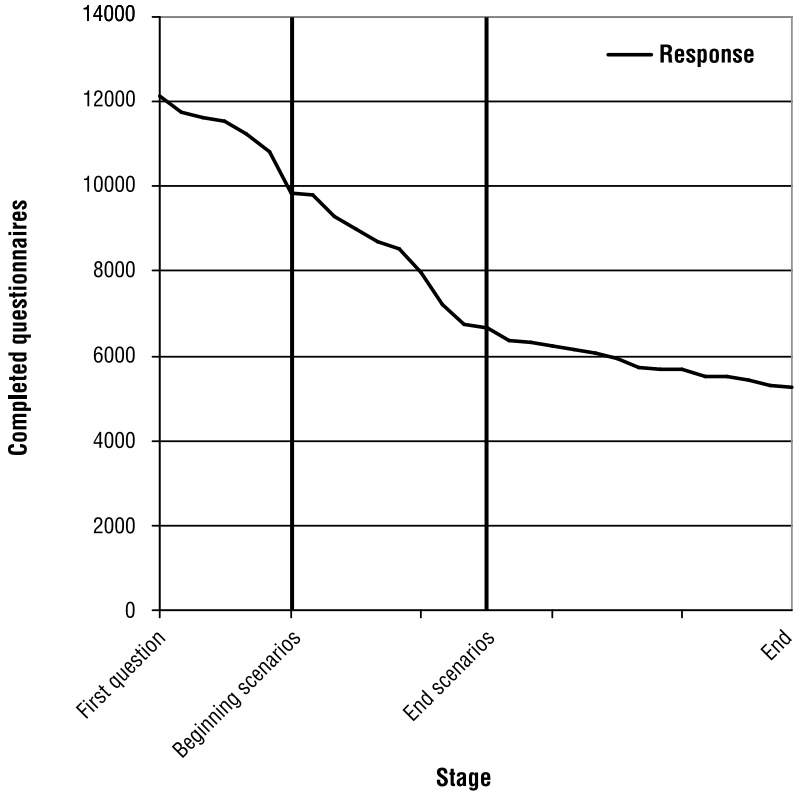
		France	UK	Spain	Germany	Total EU
Internet connection type	Broadband at home	95%	66%	80%	95%	66%
	Other connections	5%	34%	20%	5%	34%
Internet length of use	< 1 year	3%	5%	3%	3%	5%
	1-3 years	14%	20%	13%	14%	20%
	3-5 years	22%	19%	23%	22%	19%
	+5 years	61%	56%	61%	61%	56%
Surf online	Several times per day	85%	64%	80%	85%	64%
	Once a day	10%	26%	11%	10%	26%
	A few times a week	5%	9%	8%	5%	9%
	Less than once a week	0%	1%	2%	0%	1%

However, in terms of internet penetration, use and mode of connection however, figures are largely in line with official statistics, if anything somehow more generous in depicting young people as tech-savvy.

Drop-out rate

In addition to 5,265 fully completed questionnaires, 6,878 questionnaires were partially completed (Table 8).

Table 8 Drop out over questionnaire progression



An analysis of drop-out rates and question efficacy is presented below to assess the viability of survey scale-up. We present in the table below the drop-out rate question by question (Table 9). Overall, there is no large drop out for a specific question which implies that no question is problematic in se. We lost between 0.27% and 10% of response to each question. Even if this range looks significant, results are standard considering the length of the questionnaire. Questions 11 and 16 to 18 have the largest drop out rates. Question 11 is the first common question after questions specific to each scenario (q7 to q10) so the result is not surprising.

As the scenario is a vital part of the questionnaire, solutions are sought to improve the administration, for instance pictures or videos. Different presentations of scenarios should be tested before developing a larger study in other European countries. Questions 16 to 18 are about potential characteristics, benefits and risks of scenario eID system presented. It is not surprising that there is a significant drop for these questions as there are very cognitively expensive and close together. The drop out for question 17 is higher than for question 16 (9.5 vs. 6.4) which may be explained by the format of the answer (yes/no for question 16 and Likert scale for question 17). However, the drop out rate for question 18 is similar as the one for question 16. Therefore redundancy and scale format both impact on the drop out rate, and will need to be rectified (consolidated, simplified) in future studies.

Table 9 Drop out rate question by question (except scenarios)

Question	Answers	No responses	Global loss	Loss by question
1	12,143		0%	0%
2	11,732	411	3%	3%
3	11,636	507	4%	1%
4	11,527	616	5%	1%
5	11,263	880	7%	2%
6	10,834	1,309	11%	4%
11	9,783	2,360	19%	10%
12	9,298	2,845	23%	5%
13	8,992	3,151	26%	3%
14	8,681	3,462	29%	3%
15	8,515	3,628	30%	2%
16	7,969	4,174	34%	6%
17	7,208	4,935	41%	10%
18	6,743	5,400	44%	6%
19	6,674	5,469	45%	1%
20	6,351	5,792	48%	5%
21	6,333	5,810	48%	0%
22	6,157	5,986	49%	3%
23	6,082	6,061	50%	1%
24	5,935	6,208	51%	2%
25	5,717	6,426	53%	4%
26	5,697	6,446	53%	0%
27	5,673	6,470	53%	0%
28	5,534	6,609	54%	2%
29	5,519	6,624	55%	0%
30	5,428	6,715	55%	2%
31	5,308	6,835	56%	2%
32	5,265	6,878	57%	1%
33	5,265	6,878	57%	0%

Table 10 Drop out rate for scenario questions

Question	6	7	8	9	10	11
Answers	2,708	2,407	2,421	2,478	2,553	9,783
No responses		9,736	9,722	9,665	9,590	2,360
% of loss		11%	10%	8.5%	5.5%	

This is consistent with pre-test results; in case of face to face administration, due to higher cost of dropping out (interviewer presence), we suggest consolidating rather than simplifying the level of measurement (i.e. Likert scale). In the actual questionnaire, many questions remain dichotomous limiting variance and consequently precise analysis of the data (even with modern multi-scaling techniques). We also consider proper to include in future larger survey a test of different levels of measurement in the pre-test (Likert scales for fewer items vs. dichotomous for more).

The number of full answers for each scenario (questions 7 to 11) ranged between 2,407 and 2,553. The number of respondents per scenario is homogeneous: 2,407 answers for scenario Claudia, 2,421 for scenario Alice, 2,478 for scenario Alex and 2,553 for scenario Max. This is sufficient to examine overall differences between scenarios (internal validity). We also obtained more than 300 people per scenario in each country; normally n=400 considered the threshold for robust statistics in relation to validity and reliability. 300 people in each country may be adequate for the aims of an exploratory study.

Overall, scenario 4 induced less drop-out (6%) than scenarios 1 and 2 (around 11%), with scenario 3 in between (8%). We can conclude that the questions on the scenario, whether specific to each one (questions 7 to 11) or not (questions 16 to 18) effectively caused a higher drop-out rate than other questions as there were questions somewhat difficult to answer. Nevertheless, the drop out rate for scenario 4 (6%) is not very different from the one to q20, another long, complicated question. Long and difficult questions effectively caused dropt-out so this point has to be considered for the sample size in order to be able to make useful comparisons.

Completed vs. partly completed questionnaires

Table 40 (Appendix) shows a comparison of the respondents' answers on several questions. Full and partial questionnaire responses are presented for each item. The two samples are relatively similar during the unfolding of the questionnaire. Full respondents are mainly for France UK and Germany (implying a problem in Spain, as it was noted) and use the Internet for more than 5 years. They are somewhat more concerned about their identity and have a medium or high innovativeness level. On the contrary, partial respondents are slightly more reluctant to adopt eID system proposed by the central government. However, Internet trust level, informational privacy concerns and the attitude toward adopting the proposed eID system are the same in the 2 sub-samples, which is quite reassuring as the are important variables for intention to adopt eID systems. Further analysis should be conducted to understand why people dropped out. For example, the questionnaire may be tested in small-scale face-to face interviews in each country, to understand the motivations of people in dropping out: formulation of the questions, sensitiveness of the topic, length of the questionnaire, relevance, redundancy, overall coherence.

3. Survey results

In this part we present data analysis results through five areas corresponding to different parts of the questionnaire. As mentioned in the methodology, results refer to all respondents to each question. We organize the results on the main following topics:

3.1. ICT adoption and use (Q1 to Q5), knowledge of eID systems (Q19 and Q20) and innovativeness (Q6)
3.2. Attitudes toward personal data protection (Q21, Q23, Q24, Q26, Q27, Q29, Q32) and protection laws (Q30 and Q31)
3.3. Personal data handling behaviours (Q22, Q25 and Q28)
3.4. E-service scenarios (Q7 to Q18)
3.5. Case study on gender and eID

3.1. ICTs adoption and use

Young EU citizens are Web experts and connected mainly at home using broadband. Many use the Internet several times a day. Consequently, they constitute a specific part of the population particularly Internet minded. Three different groups comes out in terms of activities, a first group (48%) new Internet users doing old and classical Internet activities (check emails; search engines); a second group (34%) of older Internet users also having web 2.0 activities on social networks; a third group (18%) using all the social possibilities of the Internet such as keeping a blog and participating in online discussion forums and chats.

Internet expertise and mode of connection

Overall, 63% of all young people have used the Internet for more than 5 years. This figure is lower in Spain (56%) and higher in UK (74%) where the great majority youngsters are Internet experts. Moreover, more than 75% of the respondents connect to the Internet several times a day. However, in Spain 26% of the respondents still connect once a day.

In terms of mode of connection (Table 11), 84% of respondents connect to the internet using home broadband, then at work (30%) and at school or university (26%). Few connect to the Internet using home dial-up (12%), pay wi-fi

Note on interpretation of results, please read

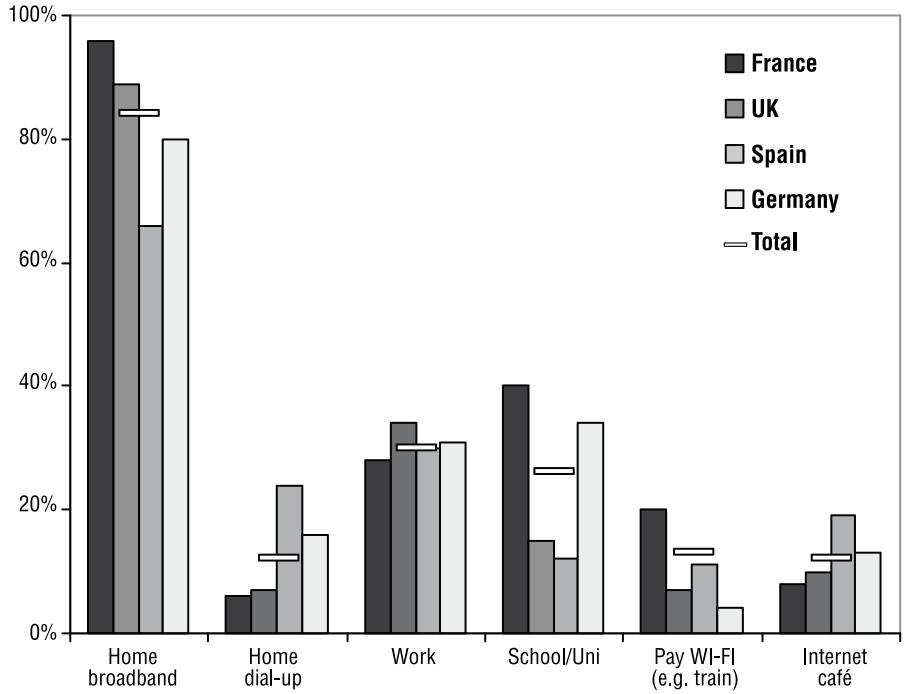
Unless otherwise specified, results are based on all available responses for univariate analysis (such as frequencies, means, etc.). Similarly, cluster analysis is based on all available responses.

For variables (e.g. trust in the Internet) measured by scales (e.g. 5 = strongly trust to 1 = strongly distrust), the mean (or average) value is reported. In general, the higher the mean, the more positive the attitude. All differences discussed in text and flagged in bold in tables are significant at $p < 0.05$. This means that results are unlikely to be due to chance. High significance is normal in studies involving large samples.

Factor analysis, correlation analysis and analysis of variance based on these draw on completed responses only (n = 5265). Factor analysis is a statistical technique that allows grouping together similar variables in one or more underlying indicators (called factors). In factor analysis tables, we provided relevant labels for these overall indicators and reported the 'factor loadings'. The bigger the 'factor loading', the closer the link between a variable and the overall indicator (e.g. the more it 'belongs').

Determination of the nature and number of factors is based on preliminary dimensional screening of variables, with special care for dichotomous items. Eigenvalues > 1 and scree plot examination are used jointly to determine the number of factors.

Table 11 Type of Internet connection by country



networks (13%) or in an internet café (12%). The situation varies among countries. In France, 95% connect using home broadband, but 40% also connect at school or university and 20% through pay wi-fi network, while very few in an internet café. In the UK, 34% connect at work but only 15% at school or university and very few in other ways. In Spain, only 66% connect using home broadband, 24% using dial-up and 19% in an internet café. The situation of Germany is quite similar to the one in France.

Country differences may be explained by the different situation of national networks, broadband being more spread in France, Germany and UK than in Spain. Differences between countries concerning universities and school equipments also explain the results.

In term of connection devices, 63% of all respondents use personal desktop PC, 55% use laptops and only 27% a shared desktop PC. Mobile phone or PDA using GPRS / 3G only accounts for 13% of the answers. This situation is due to the fact that fewer people connect to the internet through gaming consoles, even youngsters. The situation is rather similar between countries, with the exception of Spain where laptop computer connection is lower (41% of the respondents).

Internet activities

In terms of activities, nearly 100% of the respondents in all countries check email and use search engine on the Internet. A majority also use instant messaging (70%) while the fourth usage is using web sites to share pictures and videos (49%). Some discrepancies appear between countries; 85% of French youngsters use instant messaging (more any other country); 57% of Germans share videos, higher than in France (48%) and UK (45%).

An important use is managing profile on social network (43%),[23] although this is less widespread in Spain (30%). French young people

23 According to a 2007 Pew survey [http://www.pewinternet.org/ppf/r/198/report_display.asp], 55% of Americans between the ages of twelve and seventeen use some online social networking site.

author more blogs (35%) than people in other countries (<15%). Fewer youngsters design a web site or install plug-ins in all countries, except Germany for plug-ins (27%).

These more or less advanced Internet activities can be combined in 3 different factors (Table 12). The first factor corresponds to social networking and web 2.0 activities; the second to one-to-one, advanced communication activities; the third to classic Internet activities, emailing and information searching. If we divide the respondents in 3 clusters based on the Internet activities they prefer, we find that 4 activities (on 11) make the difference between the clusters. The first cluster (48%) represents new Internet users who only do old and classical Internet activities. The second cluster (18%) represents people who use all the social possibilities of the Internet such as keeping a blog and participating in online discussion forums and chats. The third cluster (34%) represents older Internet users who also use social networking sites and sites to share pictures and videos. Different people belong to these clusters (Appendix, Table 42). Cluster 1 (old Internet activities) mainly contains young (15-18) men from UK and Spain who live in rural zones. They have been using the Internet for less than 3 years and use it every day (as they are just discovering all its potentialities). Cluster 2 (communication activities) mainly contains young French female aged 19-21 who live in urban zones. They have been using the Internet for more than 3 years and use it less than once a day. Cluster 3 (social networking activities) mainly contains young people aged 22-25 from UK, Spain or Germany living in metropolitan zones. They have been using the Internet for more than 5 years and use it less than once a day.

Knowledge of eID technologies

There are significant differences in respondents' knowledge about eID technologies: PIN and password top the chart, biometrics are relatively well understood, while RFID and electronic signatures appear to baffle young users.

Of all eID technologies people claim they know, PIN/password is the most valued pass-par-tout to a range of services (Table 14). However, there is significant specialization: biometrics are the most favoured tool to access physical spaces, IP address comes second in relation to Internet identification, and electronic signature comes second for e-commerce. RFID was the least favoured tool. This may be due to improper tagging ('RFID product tracking technology') in the question definition stage.

Table 12 Factor analysis of Internet activities

	Factors		
	SNS	**Advanced individual**	**Basic**
Use website (flicker, Youtube) to share pictures, videos, movies etc	0.66		
Manage your profile on a social networking site such as Facebook	0.61		
Keep a web-log (or what is called a Blog)	0.56		
Instant messaging	0.53		
Use peer-to-peer software to exchange movies, music, etc.	0.47		
Participate in chat rooms, newsgroups or an online discussion forum	0.43		
Make or received phone calls over the Internet		0.70	
Install plug-ins in browser to extend its capability		0.68	
Design or maintain a website (not just a blog)		0.55	
Use a search engine to find information			0.74
Check email			0.65

Table 13 Knowledge of eID technologies

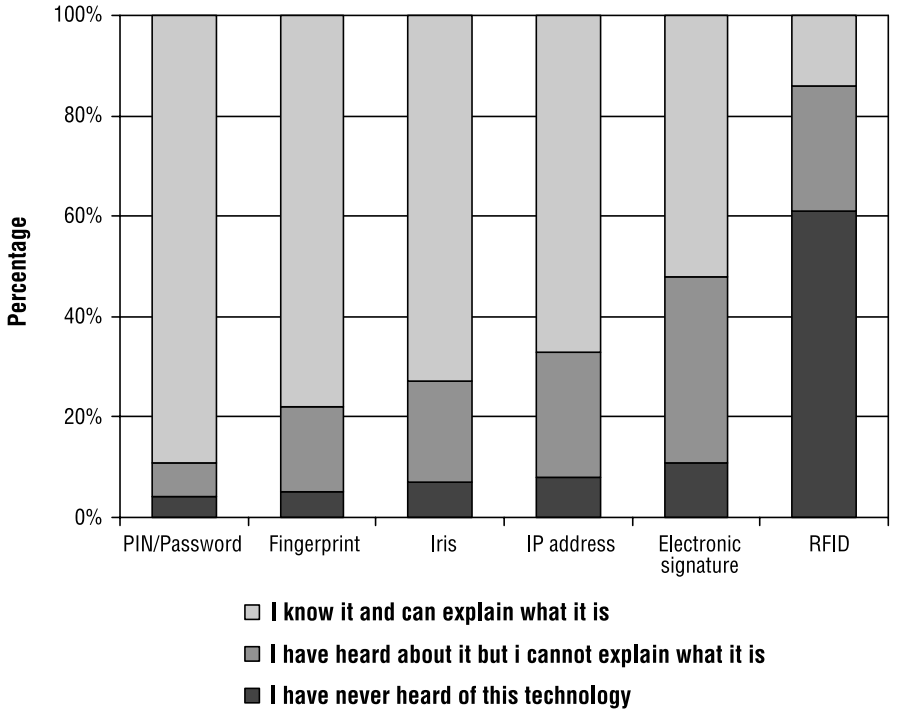


Table 14 Forecast of future uses of eID technologies for different purposes

	Access to personal devices e.g. mobile phone	Access to shared information spaces e.g. social networks	Access to remote services e.g. e-commerce	Access control to physically monitored/ restricted spaces	Access to non-remote services e.g. cash machine	None
PIN / password	82%	70%	63%	41%	65%	2%
Fingerprint	39%	18%	39%	63%	51%	6%
Eye recognition	22%	14%	32%	61%	43%	8%
Electronic signature	28%	37%	55%	25%	27%	12%
IP address	31%	60%	47%	19%	11%	16%
RFID	29%	13%	26%	34%	16%	22%

Innovativeness

Overall, young Europeans appear keen on new technologies and willing to experiment with them. Three items were used to measure people's innovativeness – reflecting propensity to experiment, to adopt early and intention to do so. These items form a single factor of 'innovativeness', with high construct reliability (Cronbach's alpha = 0.84). People's innovativeness (Appendix, Table 43) depends on nationality (English and German less innovative than French and Spanish), female gender (less innovative), and length of Internet use (more innovative) but not on age (15-25). Therefore, we suggest that any further benchmarking exercise will need to include a measure for innovativeness alongside traditional measures of technology adoption (in this case eID).

3.2. Personal data protection

Young EU citizens are sceptical about the Internet and reveal high perceived privacy risks. They make a clear distinction between personal data and identity, and attribute the responsibility to protect personal data more to themselves than to governments, which they overall distrust for this task.

Internet confidence

Most young people are sceptical of the Internet as an environment for the exchange of personal data (Table 15). Major doubts exist in relation to the protection of personal data, whereas views are more balanced on infrastructure safety.

All these items measure the same construct, named Internet security, with satisfactory reliability (Cronbach's alpha = 0.89). Perception of Internet security is largely similar in all countries, although we observe slightly higher scepticism in Germany. It also depends on all demographic variables included, age, gender, occupation and education and on 'Internet use' variables with a higher level of trust for young French people aged 15-18 living in urban zone and using the Internet for more than 5 years.

Risks in relation to personal data

Young Europeans are significantly concerned about a range of possible privacy consequences of the spreading of personal data. They are mostly concerned about stealth use, improper sharing and financial misuse of their personal information. They are less concerned about their reputation and the degree to which companies have information about them (Table 16).

While data based on adults in the US, Canada, UK, France, Germany and Japan[24] reveals that 52% of the general public surveyed feels their personal information on the Internet is kept private, only 27% of our young people perceive the same. In the study mentioned, the highest privacy concerns are of two types: advertising/spam and identity theft/protecting personal information. In our study, the second element (identity theft, protecting personal information) is of highest concern.

There seems to be a paradox: while 82% are very concerned that personal information is used without their knowledge, only 61% say that they are very concerned that companies possess private information about them. Possibly, this lies at the hearth of a 'disclosure' puzzle that we discuss later in the report.

Items measuring privacy risks and concerns can be divided in two categories (Table 17). One deals with personal data (data tracking concerns) and a second deals with identity and

24 Rosa, C. D., et al. Sharing, Privacy and Trust in Our Networked World. Dublin, OH: Online Computer Library Center, 2008. Available from <http://www.oclc.org/reports/pdfs/sharing.pdf>.

Table 15 Internet confidence

	Mean	% Agree
The internet provides a trusted environment in which to make transactions for leisure, work and business	3.94	38
In general, the internet is now a robust and safe environment in which to transact	3.59	30
The internet is safe enough to preserve my privacy as I carry out leisure, business and personal activities	3.57	29
I am confident that I can protect my privacy online	3.44	27
The internet has enough safeguards to make me feel comfortable giving my personal details online	3.33	27
Note: The scale ranks from Strongly agree (7) to Strongly disagree (1). Standard deviation is in the order of 1.67		

Table 16 Perceived privacy risks

	Very or somewhat concerned %	Neither concerned nor un-concerned %	Not very or not at all concerned %
My personal information is used without my knowledge	82	12	7
My personal data is shared with third parties without my agreement	81	13	6
I may be victim of financial fraud online	79	14	8
My identity is reconstructed using personal data from various sources	75	17	8
My identity is at risk of theft online	74	17	9
My views and behaviours may be misrepresented based on my online personal information	69	21	10
My personal safety may be at risk due to online personal information	65	21	14
My reputation may be damaged by online personal information	62	23	15
Companies possess information about me that I consider private	61	21	8

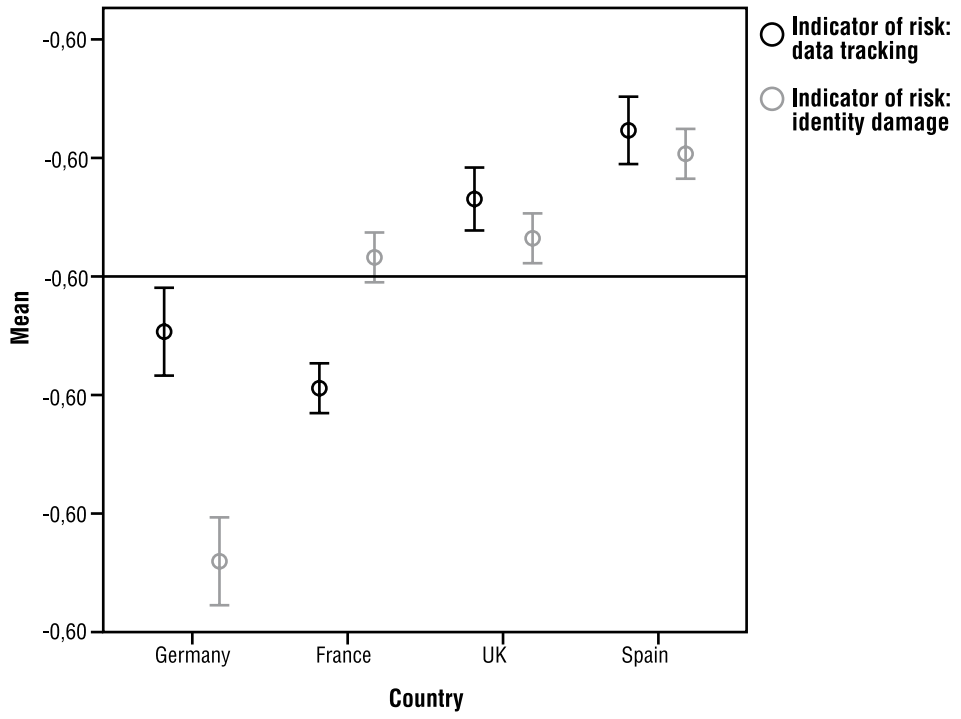
Table 17 Factor analysis of perceived privacy risks

	Factors	
	Data tracking	Identity damage
My personal data is shared with third parties without my agreement	0.81	
My personal information is used without my knowledge	0.80	
My online personal data is used to send me commercial offers	0.76	
Companies possess information about me that I consider private	0.72	
My behaviour and activities can be monitored online	0.70	
My identity is reconstructed using personal data from various sources	0.67	
My reputation may be damaged by online personal information		0.83
My personal safety may be at risk due to online personal information		0.82
My identity is at risk of theft online		0.81
My views and behaviours may be misrepresented based on online personal information		0.75
I may be victim of financial fraud online		0.69

financial fraud (identity damage concerns). Both factors measure the underlying concept with satisfactory reliability (Cronbach's alpha = 0.90). This confirms results from focus groups about the difference people made between personal data and identity. Moreover, these concepts are strongly correlated between them (Pearson's = 0.64, p= 0.001) and with Internet trust (Pearson = 0.205, p= 0.001). People who trust the Internet as a safe environment are also less concerned for their privacy and identity. As trust in the Internet is strongly correlated with privacy and identity concerns, actions in order to improve the safety of the Internet will also decrease public privacy concerns. Reassurance on the negative consequences of the spreading of personal data may also be needed.

Finally, we note that there is no clustering of items for risks in relation to online vis-à-vis offline activities. This means that young people see a continuum of risks to personal data and identity spanning virtual and real world.

Table 18 Perceived privacy risks per country



Error Bars: 95% Confidence Interval

Concerning country difference, UK and Spanish youngsters are the most sceptical concerning the use of personal data either by private companies or without their knowledge. In these two countries they are also largely more concerned by the use of personal data for commercial offers. As Table 18 suggests (difference between means of different risks by country), both risks are perceived more highly higher in Spain and in the UK than in any other country. What is more, they are seen as equally important in these countries, with data tracking a little more worrying. On the contrary, French young people are mostly concerned about identity damage, less by tracking. Germans perceive the least risks, especially in relation to identity damage.

Overall, therefore, the survey confirms this scepticism concerning the safety of Internet and privacy. Concerning privacy, our results are consistent with numerous studies having concluded that the overwhelming majority of people are 'concerned' or 'very concerned' about threats to their privacy while online and are willing to act to protect it.[25]

Elements encouraging the use of eID systems

Several elements would encourage the use of eID systems, such as assurance of respect of laws on data protection and information on the use of data. The overall message is that young people want some degree of assurance that their online transactions are technically safe and preserve their personal data privacy. Situation differs among countries: in France 71% of the respondents insist on guarantees, and 65% on labels or logos providing that the system is secure. In Germany, the first element coming out is guarantee (67% of the respondents) while 34% quote labels or logos, this difference being significant (significance of Chi2

25 C. Paine, U. D. Reips, S. Stieger, A. Joinson and T. Buchanan, "Internet users' perceptions of `privacy concerns' and `privacy actions'," International Journal of Human Computer Studies 65.6 (2007).

Table 19 Factor analysis of elements encouraging the use of eID systems

		Factors	
	Yes %	Guarantees	Control
The assurance that law on personal data protection is respected	72	0.80	
Guarantees that data are not resold or reused by another organization	69	0.79	
A label or logo proving that the system is secure	52	0.66	
A single record with all my transactions, interactions, traces, so I know what is around about me	49	0.47	
A receipt after you have provided the information	49		0.82
Information on the identification system	54		0.65
Information on the use of the data you provide	59		0.59
Testimonials of persons having experimented the system	42	**Excluded as loadings minimal**	

Table 20 Efficiency of protection methods

	Very efficient [%]	Efficient [%]
Find better technical solutions that preserve users' privacy and safety	46	41
Require that service providers take greater care of customers' identity	39	42
Make greater use of warnings and signs to signal unsafe behaviours	39	44
Set up clear guidelines for safe identity management online and offline	34	48
Raise awareness of the implication of unsafe identity behaviour	34	46
Provide formal education on safe identity management	27	47
Allocate more resources to monitoring and enforcing regulations	24	54
Give users more direct control on their own identity data	21	53

< 1%). In Spain (37%) and UK (35%) testimonials are less popular than in other countries (Chi2 < 1%). Two dimensions were extracted, which demonstrates that a range of protection methods are different in the eyes of young people (Table 19). Specifically, a first category of elements (guarantees) can encourage people in adopting new eID systems: direct guarantees, labels and logos proving that the system is secure and that no data will be misused. The second element (control) refers to user control information given to public or private authorities. The call for guarantees is stronger than the call for more personal data control mechanisms.

We then clustered respondents in three categories (Appendix, Table 45), according to propensity to favour one over the other, or both. We wish to flag here the link which emerged between the clusters and the general concept of innovativeness, discussed above; more innovative people want specific forms of protection, while all do for technology laggards (with a preference for guarantees). A strategy may involve promotion of new eID systems toward innovative people who will try the systems and convince other later adopters to use them.

Efficiency of protection methods

Young people, more than 70% of the respondents, think there are a number of efficient solutions to identity-related problems online (Table 20). Technical solutions are favoured, alongside other supply-side solutions. While half of the respondents said they are confident they can protect their own privacy online, 73% claim that it is efficient to 'give users more direct control on their own identity data'.

Table 21 Factor analysis of perceived efficiency of privacy protection

	Factor	
	Awareness raising	**Direct intervention**
Raise awareness of the implication of unsafe identity behaviour	0.83	
Set up clear guidelines for safe identity management, online and offline	0.82	
Make greater use of warnings and signs to signal possible unsafe behaviours	0.75	
Provide formal education on safe identity management	0.74	
Allocate more resources to monitoring and enforcing existing regulations		0.79
Give users more direct control on their own identity data		0.72
Require that service providers take greater care of their customer's identity		0.71
Find better technical solution that preserve users' privacy and safety		0.58

There seems to be a paradox: while half of the respondents said they are confident they can protect their own privacy online, only 21% claim that it is very efficient to 'give users more direct control on their own identity data'. While most people believe that it is either their own responsibility, they seem to admit that many users do not have the knowledge to do this effectively. Possibly, user's control on data becomes more efficient in the framework of wider, internet-level and marketplace-level data protection regulation, as is suggested by factor analysis.

Indeed, the suggested protection methods belong to two distinct categories, (Table 21). The first (awareness raising) includes educational and informational methods (e.g. warnings and signs, education …). The second (direct intervention) refers to governments' actions to enforce regulation and user control (more resources, more user control, and pressure on service provider).

Trust in handling / processing of own personal data by different agents

Young people trust their friends and family most in relation to the management of their personal identity data (Table 22). To some degree they also trust companies they know. They least trust unknown companies and non-profit associations. Known companies inspire more confidence than governments or European Union which are trust by 32% of the respondents. In France and Germany, local council, national government and European Union obtain better results than in other countries (Appendix, Table 47).

These agents are not equivalent: we distinguish 3 different types of agents based on the trust people have in them. The first type corresponds to public institutions, the second one to unknown organizations and the third one to institutions or persons close to the respondents. The third category is the most trusted and the first one the less preferred. Three groups of people also appear via cluster analysis: a first group (22%) trusting public authorities in ensuring the security and privacy of personal data; a second group (28%) not trusting public authorities at all; a middle group (50%) is sceptical regarding the capabilities of public authorities in managing the security and privacy of personal data.

Our results strongly confirm data produced in 2006 by the FIDS Network of Excellence.[26] They found that in most European Countries the strongest negative attitude was found in the judgement of ability to assess the benefits and risks when giving personal data to ID authorities. These respondents did not believe that the authorities involved in the ID card project would

26 Backhouse, J., and R. Halperin. "A Survey on Citizen's Trust in Id Systems and Authorities." Fidis Journal 1.Online (2007). <http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf>.

Table 22 Trust in institutions regarding data protection

	Mean	Factors		
		Institutions	Unknown companies	Known entities
The national government	2.81	0.92		
The European Union	2.89	0.88		
The local council	3.02	0.80		
An unknown company	1.82		0.85	
A non-profit association	2.61		0.76	
A friend, member of family	4.42			0.84
A company I am familiar with	3.27			0.68
A well-known company	2.91			0.57

Note: The scale spans from 'very much trust' (5) to 'not trust at all' (1). Standard deviation between 0.9 and 1.3.

Table 23 Knowledge of data protection rights by country

	France %	UK %	Spain %	Germany %	Total %
I never heard about them	16	8	18	7	13
I heard about them but don't know them really	39	27	26	33	32
I know a little bit about them	38	47	42	52	43
I know them well	7	18	14	8	11

be able to protect their personal data. This feeling is strongly confirmed by our study. Also, it links strongly to the finding presented above in relation to 'procedural fairness' in handling of own personal data by controllers. Young EU citizens do not trust governments or public institutions to manage personal data.

The new idea that comes out in our report is that neither public institutions nor private well known companies nor non profit association are trusted, people prefer to trust friends or themselves. Distrust of public institutions should be explored in more depth. Youngsters may fear to be monitored; youngsters are probably less confident with public institutions as they do not clearly realize the benefits and perceive more control than protection. Also, a partnership between public institutions and a well known company (as a third party) could be a possible solution.

Knowledge and opinions about data protection rights

The majority of the youngsters surveyed know just a little bit about their rights in term of data protection and one third do not really know them. In UK and Germany respondents know more than in Spain and France (Table 23). This is in line with previous studies on the lack of awareness concerning the current legal mechanisms of data protection.[27]

Despite the relative lack of knowledge, young people maintain that personal data are not properly protected (Table 24). Youngsters are not confident with public authorities if problems with data protection emerge. Factor analysis shows a single dimension of beliefs regarding data protection (in Appendix, Table 46). These items measure the same construct 'perceived

27 Gallup, Data Protection in the European Union - Citizens' Perceptions.

Table 24 Perception of personal data protection rights in own country

	Agree %	Disagree %
In [country], my personal data are properly protected	38	40
EUROBAROMETER	61	37
[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	23	51
EUROBAROMETER	41	48
I believe that the systems used by the public authorities to manage the citizens' personal data are technically secure.	30	46
I believe that citizens will be able to keep a good level of control over their personal data	23	53
I will always be able to rely on public authorities for help if problems arise with my personal data	22	57
I believe that the authorities that manage my personal data are professional and competent	26	50

public protection' with satisfactory reliability (Cronbach's alpha = 0.88).

Overall, there are three main clusters of people concerning personal data protection (Appendix, Table 48). A group of 22% trust public authorities in ensuring the security and privacy of personal data. However, 28% strongly distrust public authorities. About 50% are mildly sceptical concerning the capabilities of public authorities in managing the security and privacy of private data.

What is striking is the lack of any significant relation between knowledge of own rights and perception about framework efficacy. In other words, knowing more about one's rights does not make young people more positive towards legislation's efficacy. Especially, there is a hard core of 'sceptical' young people for whom more knowledge has no effect. This is a major problem, as it implies that awareness rising may not be the solution. Possibly, the solution may lie with increased identity-enhancing and privacy-preserving technological solutions. This apparent paradox will deserve further probing in a larger survey.

Also, the solution may not be linear. The profiles of pros, sceptics and cons are different. For example, pros are mainly young (15-18) men from Germany and France who live in urban zones and have used the Internet for long. They have high Internet trust and are rather unconcerned about privacy problems. Whether they trust public authorities because they are unconcerned or the contrary should be tested in future analyses. As Internet trust, privacy concerns and perceived public protection are correlated, actions on one of these levels may also improve the people's perceptions on the others. In other words, a complex equation involving skills, self efficacy, and privacy perception needs to be constructed in relation to the efficacy of different regulatory alternatives in relation to eID.

3.3. Personal data handling

Information provided online

Name/surname, age and nationality are provided on Internet by more than 85% of respondents (Table 25). Tastes/opinions (75%), postal address (65%) and own pictures (58%) are the second type of information provided. Sensible information (bank, judicial, biometric or financial) is provided by less than 15% of respondents.

Furthermore, personal data can be grouped in four groups, according to how similar they are in the eyes of EU young people (Table 26). The first group (sensitive data) represents very sensitive personal information such as medical or judicial

Table 25 Information provided online

	Yes %	No %	Don't know %
Age	90	9	2
Nationality	87	10	2
Name / surname	86	12	3
Tastes / Opinions	75	21	4
Postal address	65	32	4
Photos of me	58	38	4
Things I do	53	40	6
Information you give on social networks such as Facebook	50	43	7
Bodily appearance	39	55	5
People I meet regularly, my friends / Membership of associations	37	57	5
Bank information (bank card number, account number, …)	30	67	3
Places where I usually go	27	68	5
ID number	13	82	5
Financial information (revenues, credits, …)	9	88	3
Medical information (social security number, …)	7	90	3
Judicial information (criminal record, …)	5	92	3
Biometric information (fingerprint, iris…)	4	93	3
NOTE: Results may not add up to 100% due to rounding.			

information that people hardly ever disclose. The second group mainly contains 'civil status' data (high disclosure) such as the name and surname, the age, the address and the nationality. The third group represents 'descriptive' data, data which describe the way the person looks like, thinks and behaves (advanced SNS). The fourth group represent 'social' data, data that are given on social networking sites or activities (basic SNS).

When we try to gather respondents in categories based on the types of information they accept to give on the Internet, 2 main clusters appear (Appendix, Table 53). On all possible types of information, only 6 make the difference between the 2 clusters. While almost every body accepts to give 'civil status' data and dislike to give sensitive data (such as medical information), basic and advanced SNS information is a clear differentiator between two clusters, a general one and one including people oriented towards SNS disclosure.

People in cluster 1 (General) are mainly young men from France and Germany who live in rural zones (Appendix, Table 54). They have used the Internet for less than 3 years and have low Internet trust. They are very concerned by their informational privacy. On the contrary, people in the SNS cluster are mainly young women from UK and Spain who live in urban zones and use the Internet for more than 3 years. They accept to give 'social networking' information because they have low information privacy concerns. Therefore, SNS behaviour marks a watershed in the willingness to provide personal data. The survey confirms that social networkers, particularly younger users, may well be ill-informed about the detail they are making publicly available, as it is often unrelated to their privacy concerns.[28] In addition it finds

28 R. Gross and A. Acquisti. Information Revelation and Privacy in Online Social Networks. Paper presented at the Privacy in the electronic society, Alexandria, VA 2005. Available from <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>.

Table 26 Factor analysis of information provided on the Internet

	Factors			
	Sensitive data	**High disclosure**	**Advanced SNS**	**Basic SNS**
Judicial information (criminal record, …)	0.80			
Medical information (social security number, …)	0.79			
Biometric information (fingerprint, iris…)	0.77			
Financial information (revenues, credits, …)	0.74			
Bank information (bank card number, account number)	0.54			
ID number				
Name / surname		0.77		
Age		0.73		
Postal address		0.70		
Nationality		0.66		
Bodily appearance			0.76	
Things I do			0.73	
Tastes / Opinions			0.50	
Places where I usually go			0.48	
Information you give on social networks, e.g. Facebook				0.76
Photos of me				0.64
People I meet regularly, friends, memberships				0.47

NOTE: Results reported here are based on n = 4142, as 'Don't know' responses for all items were not computed. Similar results were obtained when 'Don't know' was recoded as 'No. (Appendix, Table 52). This was done to obtain indices usable for further analysis, to avoid missing values.

that personal data disclosure is weakly related to perceived risk of identity damage.

Finally, a rather amazing figure is that ID Number is not provided by 82% of the EU youngsters interviewed. ID number is problematic as it is contained in all the factors but never with good communality. However, cross analysis on ID number shows that there are differences by countries (sig Chi2 = 0.000). For example Spanish people mainly respond that they give their ID number. English people have responded that 'they didn't know' which can corresponds to the fact that they do not have an ID number. French and German youngsters mainly not give their ID number. Therefore, a benchmarking exercise should include monitoring in each country of online and offline identification methods, in relation to public and commercial transactions; this allows better estimation of propensity to use in multi-level perspective (provision, fruition).

Reasons for online self-disclosure

The main reason to disclose personal is to log into systems (70% of likely respondents) and to benefit from a better service. To connect with others justifies the disclosure up to a certain extent. Benevolent actions more than material incentives (gifts, money, price reductions) help to lower the bar for disclosure. Personalized commercial offers (based on profiling) are least appreciated. Spain is rather different from other countries concerning personal data handling, as respondents are keener than the average to disclose personal data for a range of reasons – for example, to receive personalised services and information (likely to be based on profiling).

Table 27 Reasons to online self-disclose: likelihood and factor analysis

	% very or somewhat likely	Factors		
		Hedonistic	Utilitarian	Functional
To enjoy, to take pleasure	34	0.80		
To make a good action, to help	47	0.74		
To receive valuable information	52	0.67		
To connect with others	58	0.58		
To save time (not to type information several times)	55	0.57		
To receive gifts or samples	44		0.88	
To receive money or price reductions	49		0.85	
To benefit from personalized commercial offers	37		0.75	
To log on securely onto a system (e.g. online banking)	70			0.82
To benefit from a better service (e.g. education, health)	65			0.65

Reasons to disclose can be divided in 3 categories (Table 27). The first category represents 'hedonic' benefits, the second 'utilitarian' (and even monetary) benefits. The third category corresponds to fruition of online services (functional). Overall, the third category is the most preferred and the second one the least preferred.

We also find some difference from the types of behaviours of young users recently portrayed in the US – confident creatives, concerned and careful, worried by the wayside, unfazed and inactive.[29] Young EU citizens seem to belong more to the concerned and careful segment than the confident and creative one. In other words, they are possibly more pragmatic, and taking less risks in the online environment.

To encourage people to adopt new identification systems, these systems should first propose added services such as more security and added possible applications (Health, Education). Secondly, they should propose 'hedonic' benefits such as the possibility to save time and to connect with others. Utilitarian and 'commercial' benefits should be excluded as there are not searched by young people; they could even provoke more damages because of the negative perceptions about them. This conclusion reinforces the idea that public organizations can propose these eID systems with success are they are not seen as vendors with commercial purposes.

Online personal data management tactics

In terms of identity management strategies, young EU citizens appear pragmatic rather than considerate. Overall, it was reported above, in line with as previous studies,[30] young people seem to be concerned about viruses, spam, spyware, hackers, access to personal information, security, identity theft. But they also update virus protection (50% always), scan data with anti spy (59% of often or always) and erase cookies (55%). On account of their web and technical expertise, young EU citizens both perceive high risk with eID systems and to some extent behave to stay safe online. However, while they hardly ever give misleading or wrong information, they do not always give a minimum of information or adopt other identity-shielding strategies. This confirms previous studies, where people are found to adopt copings tactics rather than adapting strategically to the new information environment.[31] Few people give the identity of someone else; they prefer giving

29 http://www.pewinternet.org/PPF/r/229/report_display.asp

30 Paine, Reips, Stieger, Joinson and Buchanan, "Internet users' perceptions of `privacy concerns' and `privacy actions'."

31 Z. Tufekci, "Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites," Bulletin of Science Technology and Society 28.1 (2008).

Table 28 Online data management strategies

	Always or often [%]	Sometimes or never [%]
Use dummy email account to shield my identity	84	16
Read the privacy policy of web sites[32]	69	31
Adapt my personal data so that no linking between profiles is possible	68	32
Change the security settings of my browser to increase privacy	64	36
Give a minimum of information	60	40
Use a pseudonym	58	42
Erase cookies	56	54
Use tools limiting the collection of personal data (e.g. cookie filtering)	42	58
Do not answer personal questions	38	62
Give your real identity	32	68
Check that the site has a safety badge before I enter valuable personal data	28	72
Give wrong information	13	87
Give the identity of another person	3	97

misleading information or even not answering. In relation to possible technical solutions, active strategies such as creating dummy email accounts and tinkering with own personal details are favourite strategies. Tools provided externally (such as trust badges and privacy-enhancing technologies) are significantly less popular.

Factor analysis reveals that there are 5 distinct online identity management strategies (Table 29).[33] The first (offline) included behaviours based on the PC such as using anti-virus, deleting cookies and updating software; the second (online) includes activities that regulate information collection collected, such as reading privacy policies and changing the browser's settings; the third strategy is one of shielding, including using dummy accounts and giving wrong information; the fourth strategy is related directly to data minimization, while the last one of avoidance of providing real identity. These strategies are significantly different from each other (limited cross-loadings, except for the last two strategies), and explain a significant amount of variance in the data (about 60%).

Cluster analysis shows that thee responses to personal data collections can be divided in two categories (Appendix, Table 50). The first category (42%) represents people who give their real identity and the second one people who adopt identity-shielding strategies (using a pseudonym, giving wrong information or not answering). The people (58%) who belong to each category are quite different (Appendix, Table 51).

We can note that none of the Internet variables (length of use and frequency of connexion) are significant differentiator of 'Identity Behaviour' clusters. Neither are the trust level in Internet and the concerns for Identity management. Cluster 1 (real identity behaviour) mainly contains young (22-25 years old) men from UK and Spain who live in metropolitan zones. On the contrary, people of cluster 2 (identity shielding strategies) are mainly young ladies aged 15-21 from France or Germany who have some concerns for their privacy. People with no concern for privacy tend to disclose their real identity whereas people with some concerns tend to adopt identity shielding strategies.

32 The item 'Read the privacy policy of web sites' (Q2901) may have been misunderstood as literature suggest lower figures (about 15%), given the amount of time implied [http://tprcweb.com/files/CostOfReadingPrivacyPolicies.pdf]. We suggest reviewing this question by distinguishing checking a privacy notice and reading it.

33 In further work, we may want to distinguish between motivations and resources required for adopting different strategies, such as their cost, their facility, the familiarity of the user, and psychological proximity.

Table 29 Factor analysis of personal data management strategies

	Factor				
	PC based	Internet based	Shielding	Minimization	Avoidance
Scan data with anti-spy ware	0.82				
Update virus protection	0.79				
Install operating system patches	0.74				
Use tools limiting the collection of personal data from my computer (e.g. firewall, cookie filtering)	0.68				
Erase cookies	0.66				
Use tools and strategies to limit unwanted email	0.61				
Check that the transaction is protected or the site has a safety badge before I enter valuable personal data	0.51				
Adapt my personal data so that no linking between profiles is possible		0.73			
Read the privacy policy of web sites		0.68			
Change the security settings of my browser to increase privacy		0.67			
Give the identity of another person			0.75		
Give wrong information			0.64		
Use dummy email account to shield my identity			0.54		
Give a minimum of information				0.77	
Do not answer personal questions				0.67	
Give your real identity					-0.79
Use a pseudonym					0.57

Table 30 Responsibility for online data protection

	%
It is my responsibility to protect my personal data	32
It is the responsibility of the company I transact with to protect my personal data online	27
It is everybody's responsibility to make sure personal data are safe online	26
It is the government responsibility to protect my personal data	8
It is the responsibility of the police and courts to ensure that personal data are protected online	7

Responsibility to protect personal data online

Most people believe that it is either their own responsibility to protect their data online or the responsibility of the companies they are transacting with. In Germany, the constitutional principle of 'informational self-determination' seems to be grounded on significant young people's attitudes. Only a minority attribute responsibility to governments and police / courts (almost nobody in the UK). In France, personal data protection is seen largely as transactional. The responsibility by everybody is more attributed than by government, police and courts, in the four countries. Overall, the picture is one that requires every concerned actor, including governments, to do their part in ensuring online protection of personal data.

3.4. eService scenarios

The questionnaire proposed the following four scenarios:

SCENARIOS

Your friend **Claudia** is 16 and always busy hanging around with her friends. A company offers her a service to keep in touch with her friends and know new people. To help her identify people she may like to meet and friends feeling like the same in the vicinity (bars, clubs, gym and university), the service requires some of her personal data, such as age, gender and location. The service is accessible through her mobile phone, based on the SIM card. If Claudia switches on the service her whereabouts and current activities are charted, to match other people's whereabouts. What would you recommend she does?

Your friend **Max** is 18; he moved from his village to Dublin to work in a call centre during the summer. To keep in touch with his friends and manage his new life, he needs to access his email accounts and mobile devices, and make use of a range of websites such as Facebook, Skype, online banking, paying tax online, online grocery shopping etc. As he has no internet at home, he uses a close-by internet café. The owner of the café offers him to manage all his activities (social, leisure and financial) from a single website, using a single login and password. What would you recommend he does?

Your friend **Alice** is turning 18, and is planning a 3-month trip abroad over the summer. She will carry her electronic passport to visit all the countries she has in mind. A company offers to add to the passport chip additional information of her choice, such as her travel preferences, food tastes, her digital signature, some emergency money etc. With this enhanced chip she could access a range of services without carrying around additional documents. For instance, shopping malls could advise on clothes she may like as she walks past them; travel agents may suggest additional sightseeing based on her route, and credit could be added to the card in case of medical emergency. What would you recommend she does?

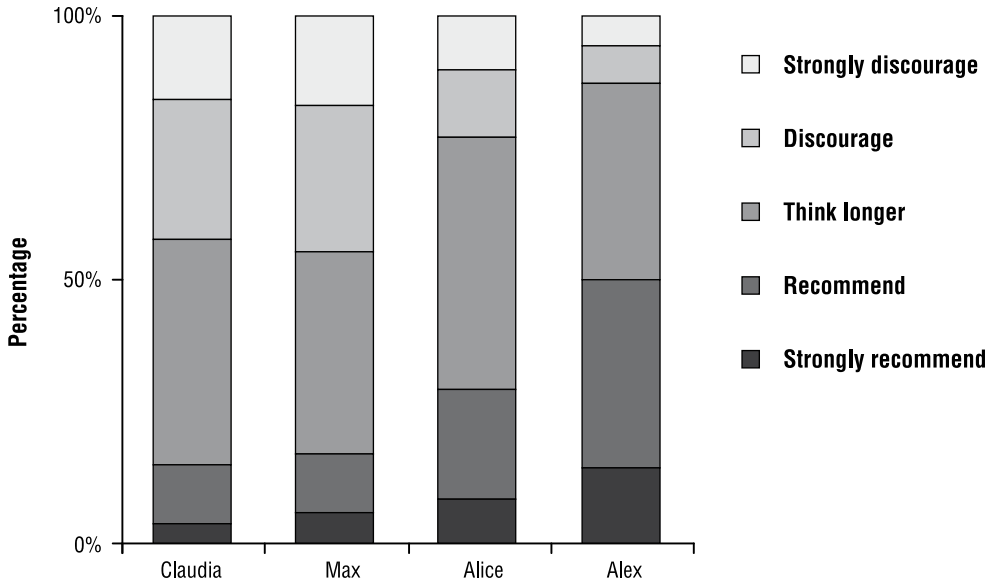
Your friend **Alex** is 17. Every day he goes to the library to practice for his driving test on one of the driving simulators provided by the local council. To enter the library he could join the queue at the counter, which is half a dozen people long, including people he knows, and have his library card scanned. In this case, the librarian will look at his file, ask him a few questions, and allocate the right simulator. Alternatively, he could use the eye-scan machine at the entrance. This automatically allocates him a simulator to use, based on his previous test results and on his preferences. The second procedure will probably take him less time. What would you recommend he does?

Forecast adoption of eServices

The scenarios were well chosen in that they represent different future alternatives. On average, the survey registered rather good perceptions on the eServices portrayed in the scenarios (42% find them a good idea, 42% like them), alongside high levels of neutral judgements (neither/nor) for all value items (good, wise, attractive, or I like the idea). The four attitude indicators were factor analysed to check the dimensionality of the concept. Results confirm that attitude toward adopting the proposed eID system is one single construct with high reliability (Cronbach's alpha = 0.91). This suggests that attitudes – negative, neutral and positive – are stable concerning eID services.

However, young people clearly like some futures better than others. Specifically, Alex (bio-enabled simulator) scores an overall positive of 53%; Alice (the connected traveller) scored 40% of positives and 35% of neutral. The situation is reversed for Max and Claudia. For Max, the positives just about outscore the negative, reflecting very mixed views single-site data control. Claudia (mobile social networking) receives far more negative appreciation (39%) than positive.

Table 31 Recommendation intentions for each scenario



Young people also clearly differentiate between them in recommending fruition (or avoidance) to friends (Table 31). Specifically, they appear to be careful about socially relevant, multi-purpose applications (Claudia, Max), and more favourable to individualized, single utility e-services (Alex, Alice).

Based on the results, the Alex scenario (access to simulator) and the Alice scenario (holiday-trip) are more likely to materialise than Max (single sign on) and Claudia (mobile social networking).[34]

Moreover, regardless of the scenario, young people urge caution (Table 32): to get more detailed information before subscribing, to wait until some friends have actually tried it and, especially for more contentious scenarios, to wait before adopting if the decision has been taken. Respondents mainly recommend waiting a little before subscribing to these eID services. Caution concerning using the service as soon as it is launched is also high, very high for Claudia and Max while Alice and Alex collect more neutral opinions. Surprisingly, in the age of 'viral marketing', recommendation by friends is less influent than more detailed information on how the system functions.

eService adoption enablers

In terms of the eServices adoption enablers (Table 33), a range of factors may encourage young users. Young people place great value on whether the service preserves their privacy (92%) and whether one can exert control on the data he submits (88%). These enablers work across all scenarios, and should have a central place in any initiative trying to promote the consumption of eServices.

The good-old free lunch is also attractive, as 86% of young people say a free service would attract them. Other possible enablers such as convenience come lower in user appreciation (83%) as does a friend's recommendation. The latter result is surprising, even if it is supported

34 The particularly positive attitude concerning biometry (scenario Alex) may be linked to influence of action movies' depiction of biometry systems (Science fiction, CIS, Matrix) in which youngsters may identify themselves with actors. A measure of media effects (cinema and games) may be added in future questionnaire.

Table 32 Additional suggestions concerning eService adoption

		Scenario			
		Claudia	Alice	Alex	Max
He/she should apply this service as soon as possible	% Disagree	64	45	31	56
	% Neither agree nor disagree	15	21	20	16
He/she should use this service soon after it is launched	% Disagree	61	47	31	53
	% Neither agree nor disagree	16	19	20	16
He/she should wait until some friends use it before subscribing	% Disagree	24	23	27	21
	% Neither agree nor disagree	14	14	16	14
He/she should get detailed information before subscribing	% Disagree	7	7	10	5
	% Neither agree nor disagree	5	4	7	4

Table 33 eService adoption enablers by scenario

	Scenario				Total	Sig.
	Claudia	Alice	Alex	Max		
If privacy is fully preserved	92%	92%	93%	93%	92%	0.78
If one can choose the personal data she wants to give	88%	89%	88%	88%	88%	0.37
If the service is free	83%	86%	**90%**	84%	86%	0.00
If the service saves time	**74%**	85%	**90%**	84%	83%	0.00
If it is very easy to subscribe	**71%**	79%	**86%**	78%	79%	0.00
If other friends strongly recommend he/she use it	67%	66%	71%	70%	68%	0.00

by the result reported previously on the lack of importance of peer trust in relation to fruition of eID systems (see Table 19). Surprise derives from the emphasis attributed in recent technical literature to distributed trust systems (peer-to-peer trust) for the consumption of online content.[35]

Overall, all the proposed elements should make the service attractive for more than 65% of the respondents for all scenarios. Different enablers matter for different scenarios except for privacy and data protection. Indeed, between 88% and 92% of respondents mention choice of data and preservation of privacy as important for all scenarios. Recommendation by friends can be a good enabler for scenarios 3 and 4 for 70% of the respondents. Proposing a 'free service' which saves time is more preferred in scenario Alice and Alex.

In relation to costs / benefits, most people judge the services sketched in the scenario as relatively easy to use, secure, and, to a much lesser degree, as a way to save money (Table 34). Young users place great value on whether the service requires a minimum of effort (60%), and makes it easier to identify oneself (60%). Overall, there is a high percentage of 'don't know' answers (16 to 32%) which probably mean that people need to see and try the system to be able to answer.

We also notice statistically significant differences in perceived potential benefits across all scenarios ($p < 0.01$). The Alex and Max scenarios are seen to require less effort than Claudia and Alice scenarios. Perceived ease of use and security are lowest in Claudia's scenario; best

35 M. Nagy, M. Vargas-Vera and E. Motta, "Managing Conflicting Beliefs with Fuzzy Trust on the Semantic Web," MICAI 2008: Advances in Artificial Intelligence, eds. M. Torres et al., "Reputation Systems for Anonymous Networks," Privacy Enhancing Technologies, vol. 5134 (Berlin / Heidelberg: Springer, 2008).

Table 34 Perceived benefits of eServices

		Scenario			
		Claudia	Alice	Alex	Max
The service requires a minimum of effort on his/her part	% Yes	52	59	67	62
	% No	15	15	12	10
	% Don't know	33	27	21	28
It would be easy to get this service to do what you want it to do	% Yes	49	53	54	53
	% No	19	18	19	16
	% Don't know	32	29	27	31
This system would enable to identify oneself more securely	% Yes	46	57	66	48
	% No	26	22	15	24
	% Don't know	28	21	19	28
This service will help one save some money	% Yes	34	43	47	37
	% No	34	29	26	29
	% Don't know	32	28	27	34
This system would provide a valuable service	% Yes	39	48	53	47
	% No	28	22	20	20
	% Don't know	33	30	27	33
This system would make it easier to identify oneself	% Yes	48	61	72	57
	% No	22	19	12	17
	% Don't know	30	20	16	26
This system would make him/her effectively control its personal data	% Yes	44	53	58	53
	% No	27	23	20	20
	% Don't know	29	24	22	27

Note: Grey shading indicates scenarios with highest perception of specific benefits

results for these variables are obtained in Alice and Alex scenarios. We also noted significant scepticism regarding the opportunity to save money in all scenarios. Perception of having control on personal data is highest for Alex and Max scenario. Overall, biometry-enabled driving simulation (Alex) is clearly perceived to carry more benefits, followed by Alice (chips) and Max (single web site). Claudia's scenario (SIM card) does not appear to provide high benefits.

Finally, concerning eService characteristics, we notice spread answers on all scales; on balance, there are rather negative views especially regarding the systems' reliability, fit with lifestyle and apparent benefits (Table 35). On the other hand, all systems appear relatively intuitive to learn and operate (more than 56% agree), across the scenarios. Discrepancies between countries are significant, as the most negative opinions are observed in Germany, the most positive in Spain. Overall, the Alex scenario involving biometry for access to personalised service attracts the most positive comments. Distrust is high for all scenarios, with a better score for biometry (Alex). Claudia consistently underperforms other scenarios on all benefit dimensions.

Dimensional analysis of three questions on enablers, benefits and characteristics did not yield any significant results. Variables load on three single construct with relatively high reliability (Cronbach's alpha ranging from 0.78 to 0.90). This may mean that scenarios are perceived as complete 'packages' rather than bundles of different parts; in other words, ease of use is very much related to fit

Table 35 eServices characteristics

		Scenario			
		Claudia	Alice	Alex	Max
Learning to use such service would be easy for me	% Agree or rather agree	56	56	59	56
	% Neither agree nor disagree	18	18	16	19
I would find this service easy to use	% Agree or rather agree	55	54	59	54
	% Neither agree nor disagree	21	21	17	21
The benefits of using this system are apparent to me	% Agree or rather agree	27	32	41	33
	% Neither agree nor disagree	27	32	41	33
I think using this system would fit well with the way I like to identify myself	% Agree or rather agree	24	30	37	29
	% Neither agree nor disagree	19	20	22	22
Using this system would fit into my lifestyle	% Agree or rather agree	23	30	36	33
	% Neither agree nor disagree	18	19	21	21
I would trust the system	% Agree or rather agree	18	23	32	20
	% Neither agree nor disagree	19	22	22	23
I think the service would be reliable	% Agree or rather agree	19	24	35	22
	% Neither agree nor disagree	24	25	25	25

Table 36 Perceived risks in relation to eID services

	Mean	Factor loadings
Someone may hack into the system and steal your personal information	5.5	0.84
Your activities may be monitored	5.5	0.74
Information may be collected that could be used against you in future life	5.2	0.82
Someone may use your identity instead of you	5.0	0.81
You will receive unwanted commercial offers	5.0	0.71
Your personal data will be shared with unauthorized persons	5.0	0.85
Your privacy may be at risk, resulting in embarrassment	4.9	0.85
You may get unauthorized charges on credit card	4.8	0.79
Your privacy may be at risk, resulting in serious personal consequences	4.8	0.85
Note: Scale ranging between Strongly disagree (=1) and strongly agree (=7). Standard deviation ranging between 1.8 – 2.0.		

with lifestyle, in turn related to system reliability. Increasing perception on one of these aspects may have a positive effect on other enablers.

Overall, results from these sets of variables suggest that the traditional convenience / privacy paradigm for the understanding of fruition of e-services may need revising so as to include a wider variety of parameters –lifestyle fit, clarity of purpose, personal data control. Interestingly, the context of consumption may matter more than previously thought vis-à-vis general attitudes towards privacy and technologies. This statement with be further elaborated in Section 3.5.

Risks associated to eID services

Young people are well aware of major risks regarding security, surveillance and negative externalities associated with the fruition of advanced e-services in converging, ubiquitous environments (Table 36). They are comparatively

Table 37 Potential risks by scenario

		Scenario			
		Claudia	Alice	Alex	Max
Your activities may be monitored	% Agree or rather agree	65	65	67	71
	% Neither agree nor disagree	10	10	14	12
Information may be collected that could be used against you in future life	% Agree or rather agree	70	67	60	65
	% Neither agree nor disagree	12	13	17	14
Someone may hack into the system and steal your personal information	% Agree or rather agree	75	74	63	76
	% Neither agree nor disagree	11	11	14	11
You may get unauthorized charges on credit card	% Agree or rather agree	56	62	43	64
	% Neither agree nor disagree	17	14	19	15
Someone may use your identity instead of you	% Agree or rather agree	70	65	42	72
	% Neither agree nor disagree	13	12	15	12
You will receive unwanted commercial offers	% Agree or rather agree	69	65	50	62
	% Neither agree nor disagree	14	13	17	14
Your privacy may be at risk, resulting in embarrassment	% Agree or rather agree	71	62	49	61
	% Neither agree nor disagree	12	15	20	16
Your privacy may be at risk, resulting in serious personal consequences	% Agree or rather agree	65	60	44	56
	% Neither agree nor disagree	15	14	18	17
Your personal data will be shared with unauthorized persons	% Agree or rather agree	68	65	50	61
	% Neither agree nor disagree	15	14	18	16

less concerned about personal safety and financial fraud. The Alex scenario of limited, biometric-based use of a relatively traditional service raises considerably less concern than other scenarios.

These perceived risks have been submitted to factor analysis to see if there are different factors. Results show that all these risks pertain to a single concept corresponding to perceived privacy risks which measure has a satisfactory reliability index (Cronbach's alpha = 0.93). Surprisingly, there are no differences between eServices in this respect. High level of risks perceived implies, in case of an eID systems deployment, analysis of elements that affect risks perceptions such as guarantees or logos showing that people's privacy will be preserved.

Again, there are differences in risk perceptions across the scenarios. Biometry (Alex scenario) presents less perceived risks (Table 37). Overall, again, trust and perceived risks may depend more on the purpose / aim of the service, and in the transaction involved, than in the underlying eID technology, in this case highly contentious biometry. This was also the most preferred scenario in terms of perceived benefits. Financial fraud is mostly feared for Alice and Max scenarios and identity fraud is feared in the Max scenario. Claudia's scenario has less perceived risks for unauthorized charges on a credit card, but high perception of other types of risks.

Specifically, while the incidence of identity theft is lower in the EU than in the US,[36] the

36 According to the Federal Trade Commission (report 2005), 9.3 million US citizens suffered identity theft in 2004, while the UK Home Office says 100,000 Britons suffered the same fate.

Table 38 Factor analysis of 'who should offer the service'

	Yes %	Factors		
		Institutions	Known company	No-profit
A government agency	25	0.79		
The central government	33	0.77		
A local authority	18	0.70		
A famous private company	27		0.78	
A company you know well	34		0.70	
A new, specialised company	23		0.57	
A non-profit company	30			0.95

problem is becoming a matter of greater concern.[37] Our study confirms high risk perceptions of identity theft. In the scenarios, 36% of the respondents feel that even with eID systems, identity theft remains a risk and 32% express the view that privacy may be at risk. Interestingly, the Alex scenario based on biometry raises the least concerns in relation to impersonations.

Overall, it appears from the analysis that trust must be seriously reinforced. Reinsurance on proper use of personal data and privacy protection is a key factor of success, but perceptions are highly negative now.

Who should offer eID services

None of the mentioned institutions obtain high scores, showing a clear lack of confidence in these institutions to manage eID systems (Table 38). Partly, this masks a possible lack of clarity in the scenarios, and highlights some of the pitfalls discussed before of discussing complicated scenarios with a survey tool. This said, people make a clear distinction between public, private and no-profit organisations as possible service providers, and even between institutions within categories. However, only 30% of youngsters agree that any of these organizations should provide eID services.

These potential service providers can be gathered in three categories. The first category represents public institutions such as a local authority. The second contains private institutions and the third one non-profit organizations. Results above show that people make a clear distinction between the categories and even between the institutions in each category.

But there are also small differences between the scenarios. People in the Alex and Max scenarios are less reluctant toward the proposed e-services providers. The Alex scenario is the one which encounters most favour toward public institutions. On the contrary, Claudia scenario is the one for which reluctance toward public authorities is highest.

Finally, this question flagged the challenges of conducting in-depth research based on survey scenarios. Focus groups or other techniques more suitable to explore latent attitudes to future services may be employed in this respect. Discussion should include other elements outside trust, such as experience with the provider, convenience to exchange data and other contextual enablers.

3.5. Adoption and risk-aversion: a profile

Next, we set to know more about those young people who rated the scenarios highly, and those who perceived very high risks in relation to service fruition. The two constructs are closely

37 http://ec.europa.eu/justice_home/funding/tenders/funding_tenders_146524_en.htm

Table 39 Correlations for eService appreciation and eService risks

		eService appreciation	eService risk	eService appreciation controlling for eService risk
Age		-0.031*	-0.043**	-0.050**
Internet length of use		-0.036**	0.082**	-0.007
SNS online behaviour		0.065**		0.071**
Individual advanced online behaviour			0.067**	0.044**
Baseline online behaviour		-0.091**	0.145**	-0.042**
Innovativeness		0.126**		0.139**
Low disclosure	C	0.131**	-0.121**	0.095**
Advanced SNS	C	0.138**	-0.041**	0.132**
High disclosure	C	0.072**		0.074**
Basic SNS	C	0.064**		0.075**
DP tactics: offline	C		0.165**	0.044**
DP tactics: online	C		0.087**	0.028*
DP tactics: minimisation	C	-0.099**	0.149**	-0.049**
DP tactics: shielding			-0.033*	-0.019
DP tactics: avoidance		-0.070**	0.038**	-0.061**
Internet trust	B	0.178**	-0.136**	0.139**
Risk: data tracking		-0.092**	0.259**	0.002
Risk: identity damage			0.133**	0.060**
Knowledge of DP rights		-0.042**	0.086**	-0.012
Attitudes toward DP	A	0.200**	-0.121**	0.168**
Policy: awareness	D	0.031*	0.094**	0.070**
Policy: intervention	D	0.103**	0.049**	0.129**
eID enabler: guarantees	D	0.069**	0.124**	0.123**
eID enabler: control	D	0.134**		0.150**

The table reports Pearson's correlation coefficients.
**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

related, the higher perceived risk, the lower appreciation of the value of the service (Pearson's R2 = - 0.36). In the first two columns of Table 39 we look at correlation between a range of factors and, respectively eService appreciation and eService perceived risk.

The table tells two interesting tales First, it flags the possible predictors of high evaluation services. The most important factor (marked A in table) is positive attitudes to data protection in own country. That is to say, the perceived effectiveness of the data protection framework is of crucial importance for the fruition of services. The second most important factor (marked B) is trust in the Internet regarding safety and privacy, again an 'infrastructural' factor important for eServices. Thirdly, those who disclose more (marked C), especially on Social networking sites, are more likely are more likely to appreciate eServices more. These people also consider themselves innovative, in terms of technology uptake. Young people endorsing novel eServices think that intervention is the most efficient measure to ensure Internet and eID services privacy and safety. Although they support guarantees, they are

ready to take a degree of responsibility for their online behaviour (marked D).

Second, analysis points to possible causes of high eService risk perceptions. One important factor remains the attitude to data protection: low perception of DP accrue to the perception of risk. Again internet trust is important, as lack of may increase the perception of risk. Here the symmetry comes to an end. In deed, risk in eServices is closely related to perceived data tacking and identity damage risk in relation to personal data in real life. It seem that unless solutions are found that abate this triangle of high risk, low trust in legal framework and internet safety, it may be difficult to persuade these people to join in novel eServices. Behaviourally, people with low appreciation of eServices engage in a more limited range of Internet activities, tend to disclose less and tend to employ strong personal data shielding strategies (blue). Finally, people who highly perceive risks call for more awareness raising n general and for guarantees in relation to eID services in particular.

To get an impression of how perceived risk affects value perception, the same analysis was run as in the first column, but controlling for perceived risks. In other words, perceived risk may moderate positive effects of enablers and reinforce negative predictor's influence. What we want to flag here is that controlling for risks, keeping it constant, that is to say, increases the importance of more regulation for the fruition of eID services, in the forms of more guarantees, control, policies promoting awareness and direct intervention.

Warning: the gender eID divide

The majority of results presented suggest that male and female young people react differently to eID systems and services. Findings correspond generally to those of the wider literature on ICTs and gender:

- Females are more sceptical about scenarios, more often recommending thinking about it for a bit longer than males.
- Regarding eID services characteristics, females are neutral and less positive than males, expressing more scepticism.
- Female respondents seem to be more influenced by recommendation by friends and by a service's lack of cost.
- Females confide more than males in non-profit companies and public institutions.
- Ease of use of the service is less important for females than for males.
- Males are more positive than females on other criteria (value for money, security)
- Overall regarding eService characteristics, females are less positive and more neutral, showing therefore a certain reluctance face to eID systems.

However:

- There are no gender differences concerning risks.
- Scepticism of females towards eID systems may be explained by less knowledge of eID technologies such as IP address and RFID.

Further analysis of this apparent eID divide is required.

4. Conclusions

4.1. Main thematic findings

Survey results give a quantitative measure of young Europeans' perceptions and acceptance of risks, general motivations, attitudes and behaviours concerning eID-enabled services. We present the main results under three headings:

Young people's perception of technologies

Digital culture and markets matter. There are significant differences between countries in terms of digital culture and markets. Spain presents lower social network usage; France has a blogging culture; youngsters are more skilled in Germany than elsewhere. Computers still rule, PC access to the Internet is still prevalent while mobile (GPRS and 3G) is only used by one in six. Even fewer connect to the Internet through gaming consoles. Internet access and activities are important for personal innovativeness, and, in turn, for the take up of eID services. Country specific differences and commonalities, particularly on youngsters' expertise and activities on the Internet, can be found in Section 3.1, page 31.

Young, innovative people, who go online via broadband several times a day for more than 5 years, are digital leaders in relation to eID. They are Web2.0 experts and this matters for the future take up of advanced eID-based services. E-mail, search engines and instant messaging are ubiquitous today, and half the respondents also engage in Web 2.0 activities (e.g. sharing pictures) and social networking sites. This behaviour often requires significant online disclosure of personal data, which youngsters are happy to provide. This attitude to adopt quickly and creatively these new services is not risk-free. Regulation has to strike a balance between encouraging the best use of innovative services and their associate risk with regard to safety and privacy. Survey results on disclosure of sensitive data, the use of services, Internet confidence and perceived privacy risk are given in Sections 3.1 to 3.3.

Young people use different eID technologies for specific purposes. PINs and passwords constitute a 'pass partout' for a range of services. Biometrics are relatively well understood as an access tool for shared physical spaces. IP is on the radar as a mean for authenticating oneself online. RFID and electronic signatures still confuse young users. Our scenarios embedding different eID technologies in plausible settings reveal that 'fit-to-purpose' eID technologies show a higher degree of acceptance. If familiarity were to be harnessed to increase eID acceptance, the context of service take up and the clarity of purpose matters more than technologies per se and than general attitudes to personal data protection. Details of the need for context-dependence and target purpose of eID technologies can be found in Section 3.1 on page 33-34 and Section 3.4 on page 47.

Gender matters. Female users are more reluctant to use eID technologies than male users. Scepticism of females may be explained partly by an apparent lower degree of knowledge of eID technologies, by a higher level of perceived risks and by lesser willingness to disclose personal data. These results confirm previous evidence on gender difference in the Internet adoption and in broadband access. Unlike these, however, take up of eID services is highly context dependent. Therefore, the case of gender-friendly eID technologies needs to be examined. More information on gender aspects are found across the whole report, and summarized on page 56 (Warning: the gender eID divide).

Privacy, trust and enablers

There are high perceptions of risks, both general and contextual. Most young people are sceptical of the Internet as an environment for the exchange of personal data and major doubts exist in relation to personal data protection. They perceive high risks on giving personal data and fear their misuse in specific eService settings. General perception of risks with respect to Internet behaviour are correlated to contextual risks reported in the eService scenarios, but do not explain them entirely. But not only: young people see a continuum of risks to personal data and identity that spans from the virtual to the real world. Risk greatly hampers the take up of eID services. A summary of the results related to risk perceptions is available in Section 3.2 on page 36 and in Section 3.4 on page 52.

There is a strong call for fair data protection rules. Trust in providers (institutions-based trust) is not a strong driver of adoption, contrary to a wealth of previous evidence. However, young people very strongly demand procedural fairness in the management of their data. Trust in rules (fair play by eID services providers) is an important factor to monitor, in addition to traditional understandings of trust (institution-based, interpersonal, systemic, contextual). Findings on trust in the handing and processing of personal data can be found in Section 3.2 on page 39. Indeed, there are multiple enablers of eID-based services. Guarantees, assurance of data protection law respect and precise information on eID systems are likely to encourage the use of eID systems. This may be accomplished through:

- overt compliance of eID service providers with data protection and privacy principles. This may include policy options or new regulations suitable for specific users' needs and requirements;
- communication strategies tailored to young people on the benefits and risks that eID services (and not only technologies) can offer. Simple or general awareness rising campaigns do not work;
- user-friendly interfaces. Young people are highly confident in their ability to use sophisticated services. Although the IT skills of the sample are high by Eurostat standards, they demand user-friendly interfaces in order to adopt eID services.

Young people's policy perceptions

Young people consider that the responsibility of the management of personal data is shared. They trust friends and family more than institutions in relation to the management of personal identity data. They do not attribute responsibility for the protection of personal data to governments or police and courts. Instead, they are asking for tools that give them more direct control of their own identity data. At the same time they do not feel very confident in their own ability to keep their data protected. Furthermore, they often neglect trust seals and do not appreciate privacy enhancing tools. Institutions need to be aware of this apparent mismatch. Current 'privacy enhancing' strategies should be expanded to 'identity enhancing' ones, which take into account young people's digital lifestyles and identity-related activities. Results on responsibility are summarized in Section 3.3 page 46.

Data protection legislation is unknown and unloved. Young EU citizens' knowledge level about data protection laws is very low. Even lower is their appreciation of the current protection framework. Paradoxically, more knowledge seems not to breed more positive attitudes. Moreover, more knowledge on data protection rights seem not to influence their propensity towards take up of eID services. Both these findings suggest that experience may matter more than understanding of the legal system. Therefore, it is not surprising

that young people should ask for 'hands-on' regulation. Young people desire reassurance, via practical tools more than via awareness raising. A first category of tools (guarantees, such as labels and logos) would encourage people to adopt new eID systems. A second set of tools would assist user control of personal data provided to public or private authorities. The call for guarantees is stronger than the call for more personal data control mechanisms, as it was identified in the previous paragraph.

4.2. Considerations for future work

A large-scale survey, as any other research tools, is only as good as the questions it wants to answer. The survey showed that the field of eID is more complex than commonly thought. It implies measuring young EU citizen's perceptions and attitudes toward Internet, toward online personal data management, toward data protection legislation and in relation to specific eID scenarios. Overall, the first item on a future research agenda is to review the questionnaire with a view of updating concepts taken from the privacy and technology acceptance model literature. eID is becoming an ever more important technological bundle, one that requires precise modelling in terms of trust, acceptance, privacy and personal data management. Any further study should focus more the eID scenarios and associated services. Different types of scenario presentations have to be formulated, validated and presented.

The study generated a number of suggestions which may help to take the results of this study further.

Further explore inter-country differences. Some commonalities appear between countries concerning high risks perception towards personal data management, global distrust towards institutions to manage personal information and reluctance to use eID systems just after their launch. This rather 'homogeneous' situation is probably due to the study limitation to France, UK, Spain and Germany, which all have developed Internet infrastructures and whose citizens are digitally minded.

There seems to be country-specific differences concerning attitude to technologies, maturity of markets, prospective uses. For instance, Spain appears to be different from other countries in terms of attitudes, slightly less mature as a market, France looks intermediate but trendy, while the UK and Germany are mature markets, in different ways. EU 'heterogeneity' has to be examined in further studies and planned for in terms of eIdentity policy. Specifically, one may want to examine additional sources of inter-country variance, such as:[38]

- Overall media environment, especially Internet diffusion, increase in access/use, risks, opportunities but also regulation frameworks (including self-regulation);
- Media coverage in different countries may give disproportionate attention to data breaches and risks rather than to benefits;
- The online role of public service providers which may encourage beneficial use.

Link to wider social trends. Clearly, this reports outlines high perceptions of risks in using Internet or eID systems in the four countries. This, in turn, is strongly related to lack of trust in public institutions concerning personal data management. Analysis of the key variables included in the increasing 'trust' literature may help to define policies. Time-series investigation is needed to better understand why and how EU citizens distrust public institutions. Investigation on possible strategies to increase trust towards new technologies should clarify the types of

38 Inspired by a presentation given by Sonia Livingstone at the Safer Internet Forum 2008 http://www.lse.ac.uk/collections/EUKidsOnline/LuxembourgSept2008.pdf

actions that should have an impact on trust. This investigation may eventually include experimentation in different countries.

Extend to multi-level analysis. The study helped to distinguish between several levels of eID:

- eID – personal perception and management of the digital self;
- eID tools and systems – tools that assist eID management, such as OpenID, Facebook;
- eID technologies – such as fingerprint, tokens and processes based on them;
- eID services – services based on eID as well as eID systems and tools.

In the current eID market, there is a blurring of lines in relation to different layers, with virtual tokens, identity meta-system, single-sign-on and other devices crossing the online and online. These are different targets for analysis, depending on what policy-makers wish to regulate; this study looked largely at eID and eID services. However, there is a need to know more about other layers; this may be object of benchmarking, useful for integration in future multi-level modelling exercises (where 'country', 'region' or 'district' are also critical levels). For instance, the survey did not include a question on eID systems and tools, such as OpenID, Card space, Facebook Connect, mobile applications; they may be included in future surveys or monitored using benchmarking. Regarding eID technologies, tokens and virtual tokens were not included; the current convergence between online and offline in terms of identity management ought to deserve more space in future studies of eID and eID-enabled services.

Consider benchmarking. The study highlighted the need for rigorous benchmarking of the state of European readiness in terms of eID. The study suggests action in three areas. The first aim should be to measure precisely the maturity difference between Member States concerning eID systems. A inter-country comparison of eID infrastructure, legal environment concerning personal data protection (type of protection, institution responsible to protect), measures of digital divide by category of population and by geographic zone, parts of existing zones in the country not connected to the Internet, passport and other eID systems, existing eID systems and usages would be beneficial. This work ('eID Scoreboard') would indicate the overall state of eID maturity of each country and would help to define local policies on data protection and eID systems.

5. Appendix 1: Final Questionnaire

The questionnaire includes information on question topic, exact question formulation, the answers available to respondents, how these answers were measured (e.g. yes/no, agree to strongly agree, etc.) and the value attributed in the databases to people's responses (e.g., 1 for yes, 7 for strongly agree, etc).

1. Internet Use

Internet length of use					
Q1		Less than one year	Between one and three years	Between three and five years	More than five years
101	**How long have you been using the internet?**	1	2	3	4

Connection place		
Q2	**How do you connect to the Internet ?**	Tick all that apply
201	Where I usually live (home, parent's home, Uni) using broadband	1
202	Where I usually live (home, parent's home, Uni) using dial-up	1
203	At work	1
204	At school or university	1
205	Through pay wi-fi network (airport, train station…)	1
206	In an internet cafe	1

Connection frequency		
Q3	**How often do you connect to the Internet?**	
301	Several times a day	1
302	Once a day	2
303	A few times a week	3
304	Less than once a week	4
305	Less than once a month	5
306	Never	6

Connection devices		
Q4	**What devices do you use to connect to the Internet?**	Tick all that apply
401	Personal Desktop PC	1
402	Shared Desktop PC	1
403	Laptop computer	1
404	WII, playstation or other gaming console	1
405	On mobile phone or PDA, using GPRS or 3G	1

Internet skills		
Q5	**Do you do the following activities on the internet?**	Tick all that apply
501	Check email	1
502	Instant messaging	1
503	Participate in chat rooms, newsgroups or an online discussion forum	1
504	Use a search engine to find information	1
505	Use website (flicker, Youtube, etc) to share pictures, videos, movies etc.	1
506	Make or received phone calls over the Internet	1
507	Manage your profile on a social networking site such as Youtube, myspace or Facebook	1
508	Design or maintain a website (not just a blog)	1
509	Keep a web-log (or what is called a Blog)	1
510	Install plug-ins in browser to extend its capability	1
511	Use peer-to-peer software to exchange movies, music, etc.	1

Innovativeness				
Q6	How would you place yourself, in relation to your peers?	Strongly disagree	To	Strongly agree
601	I am among the first to try out new technologies	1		7
602	When I hear about a new technology, I look for ways to adopt it	1		7
603	I like to experiment with new technologies	1		7

2- SCENARII

QUESTION SPECIFIC TO EACH SCENARIO (Q31 for S1, q31bis for S2, q31ter for S3 et q31quar for S4)

Potential behaviour (specific)					
Q7	**If you were Claudia, what would you do?**	Strongly disagree	To	Strongly agree	Do not know
701	Only use if the mobile has added safety, such as fingerprint recognition, voice recognition or a safe way to identity myself	1		7	8
702	I would be careful, as using the service may put safety at risk by meeting strangers	1		7	8
703	It would be useful if the service could be linked to my social networking profile, e.g. Facebook, MySpace, etc	1		7	8

Q8	**If you were Alice, what would you do?**	Strongly disagree	To	Strongly agree	Do not know
801	I would only use if the chip can be deactivated when needed, as my movement may be tracked for other purposes	1		7	8
802	I would only use the service if the data generated is destroyed as soon as I do not need it	1		7	8
803	It would be useful if this information could be available online, to update and consult	1		7	8

Q9	If you were Alex, what would you do?	Strongly disagree	To	Strongly agree	Do not know
901	I would only use the service if the system was based on fingerprint recognition, as it may be less intrusive	1		7	8
902	I would only use the service if my driving results are not used to calculate my insurance or to limit my ability to drive fast cars	1		7	8
903	It would be better if the system allowed me and my friends to share and compare our driving results	1		7	8

Q10	If you were Max, what would you do?	Strongly disagree	To	Strongly agree	Do not know
1001	The system is not secure enough, I would rather use safer technologies such as fingerprint to identify myself on the single site	1		7	8
1002	I would be careful, as having all my information in a single place may lead to identity fraud	1		7	8
1003	I would like to use a similar system based on a smart card to carry around, so I could also use it for offline transactions	1		7	8

Questions common to all scenarios

Recommendation				
Q1101	**Would you recommend that your friend subscribes to the service?**	Strongly recommend	To	Strongly discourage
		1		5

Intention of eID adoption				
Q12	**What else would you recommend to your friend?**	Strongly disagree	To	Strongly agree
1201	He/she should apply this service as soon as possible	1		7
1202	He/she should use this service soon after it is launched	1		7
1203	He/she should wait until some friends use it before subscribing	1		7
1204	He/she should get detailed information before subscribing	Strongly disagree	To	Strongly agree

Attitude				
Q13	**Overall, do you think that:**			
		1	To	5
1301	Using this service would be:	A good idea		A bad idea
1302	Using this service would be:	A wise idea		A foolish idea
1303	Using this service would be:	Attractive		Non attractive
1304	The idea of using this service	You like it		You dislike it

Adoption enablers				
Q14	**What would make the service attractive?**	Yes	No	Don't know
1401	If other friends strongly recommend he/she use it	1	2	3
1402	If the service is free	1	2	3
1403	If one can choose the personal data he/she wants to give	1	2	3
1404	If the service saves time	1	2	3
1405	If it is very easy to subscribe	1	2	3
1406	If privacy is fully preserved	1	2	3

Best service providers		
Q15	**Who do you think should offer the service proposed in the scenario ?**	Tick all that apply
1501	A famous private company	1
1502	A new, specialised company	1
1503	A company you know well	1
1504	A non-profit company	1
1505	The central government	1
1506	A government agency	1
1507	A local authority	1
1508	I don't know	1

Benefits of the service				
Q16	**What are the potential benefits you would mention to your friend?**	Yes	No	Don't know
1601	The service requires a minimum of effort on his/her part	1	2	3
1602	It would be easy to get this service to do what you want it to do	1	2	3
1603	This system would enable to identify oneself more securely	1	2	3
1604	This service will help one save some money	1	2	3
1605	This system would provide a valuable service	1	2	3
1606	This system would make it easier to identify oneself	1	2	3
1607	This system would make him/her effectively control its personal data	1	2	3

Characteristics of the service				
Q17	**To what extent do you agree with the following description of the service?**	Strongly disagree	To	Strongly agree
1701	Learning to use such service would be easy for me	1		7
1702	I would find this service easy to use	1		7
1703	I would trust the system	1		7
1704	I think the service would be reliable	1		7
1705	I think using this system would fit well with the way that I like to identify myself	1		7
1706	Using this system would fit into my lifestyle	1		7
1707	The benefits of using this system are apparent to me	1		7

Potential risks				
Q18	**What are the potential risks you would mention to your friend?**	Strongly disagree	To	Strongly agree
1801	Your activities may be monitored	1		7
1802	Information may be collected that could be used against you in future life	1		7
1803	Someone may hack into the system and steal your personal information	1		7
1804	You may get unauthorized charges on credit card	1		7
1805	Someone may use your identity instead of you	1		7
1806	You will receive unwanted commercial offers	1		7
1807	Your privacy may be at risk, resulting in embarrassment	1		7
1808	Your privacy may be at risk, resulting in serious personal consequences	1		7
1809	Your personal data will be shared with unauthorized persons	1		7

3- Knowledge and Perception of EID Systems

Knowledge				
Q19	**Do you know these identity systems?**	I have never heard of this technology	I have heard about it but I cannot explain what it is	I know it and can explain what it is
1901	PIN/password	1	2	3
1902	RFID product tracking technology	1	2	3
1903	Fingerprint recognition	1	2	3
1904	Eye recognition	1	2	3
1905	IP address [i.e. Through your internet service provider]	1	2	3
1906	Electronic signature	1	2	3

Context of use		
Q20	In what context do you think the use of these identity systems is useful?	Tick all that apply
2011	Access to personal devices (e.g. Mobile phone, PDA, car …)	1
2012	Access to shared information spaces (e.g. Social networks)	1
2013	Access to remote services (e-commerce, financial transactions, e-gov …)	1
2014	Access control to physically monitored/restricted spaces	1
2015	Access to non remote services (e.g. Cash machine)	1
2016	Other applications (e.g. eID cards)	1
2017	None	1

Enablers		
Q21	**Which of the following elements could encourage you to use identification systems?**	Tick all that apply
2101	A receipt after you have provided the information	1
2102	Information on the identification system	1
2103	Information on the use of the data you provide	1
2104	Testimonials of persons having experimented the identification system	1
2105	The assurance that law on personal data protection is respected	1
2106	A label or logo proving that the system is secure	1
2107	Guarantees that data are not resold or reused by another organization	1
2108	A single record with all my transactions, interactions, traces, so I know what is around about me	1
2109	Others (specify)	1
2110	None	1

4. Personal Data Management

Information provision				
Q22	**Indicate what information you provide on Internet**	Yes	No	Don't know
2201	Name / surname	1	2	3
2202	Age	1	2	3
2203	Nationality	1	2	3
2204	ID number	1	2	3
2205	Postal address	1	2	3
2206	Bodily appearance	1	2	3
2207	Things I do	1	2	3
2208	Tastes / Opinions	1	2	3
2209	People I meet regularly, my friends / Membership of associations	1	2	3
2210	Places where I usually go	1	2	3
2211	Information you give on social networks such as Facebook or Study VZ	1	2	3
2212	Photos of me	1	2	3
2213	Financial information (revenues, credits, …)	1	2	3
2214	Medical information (social security number, …)	1	2	3
2215	Bank information (bank card number, account number, …)	1	2	3
2216	Judicial information (criminal record, …)	1	2	3
2217	Biometric information (fingerprint, iris…)	1	2	3

Trust in mediators re personal data handling					
Q23	**Overall, how much do you trust the following people to handle your personal information safely?**	Very much trust	To	Not trust at all	Don't know
2301	A friend, member of family	1		5	6
2302	The local council	1		5	6
2303	The national government	1		5	6
2304	The European Union	1		5	6
2305	A well-known company	1		5	6
2306	A company I am familiar with	1		5	6
2307	An unknown company	1		5	6
2308	A non-profit association	1		5	6

Internet confidence				
Q24	More generally, concerning the Internet, you would say that…	Strongly disagree	To	Strongly agree
2401	The internet has enough safeguards to make me feel comfortable giving my personal details online	1		7
2402	The internet is now a robust and safe environment in which to transact.	1		7
2403	The internet provides a trusted environment in which to make transactions for leisure, work and business	1		7
2404	The internet is safe enough to preserve my privacy as I carry out leisure, business and personal activities	1		7
2405	I am confident that I can protect my privacy online	1		7

Benefits				
Q25	**How likely are you to provide personal data for the following reasons?**	Very likely	To	Very unlikely
2501	To save time (not to type information several times for instance)	1		5
2502	To benefit from a better service (e.g. Education, health, etc)	1		5
2503	To receive valuable information	1		5
2504	To enjoy, to take pleasure	1		5
2505	To make a good action, to help	1		5
2506	To connect with others	1		5
2507	To benefit from personalized commercial offers	1		5
2508	To receive gifts or samples	1		5
2509	To receive money or price reductions	1		5
2510	To log on securely onto a system (online banking, uni network, etc)	1		5

Privacy concerns				
Q26	**How concerned are you about the following risks in relation to your personal information**	Very concerned	To	Not at all concerned
2601	Companies possess information about me that I consider private	1		5
2602	My personal information is used without my knowledge	1		5
2603	My personal data is shared with third parties without my agreement	1		5
2604	My behaviour and activities can be monitored online	1		5
2605	My online personal data is used to send me commercial offers	1		5
2606	My identity is reconstructed using personal data from various sources	1		5
2607	My views and behaviours may be misrepresented based on my online personal information	1		5
2608	My reputation may be damaged by online personal information	1		5
2609	My identity is at risk of theft online	1		5
2610	My personal safety may be at risk due to online personal information	1		5
2611	I may be victim of financial fraud online	1		5

Responsibility for personal data safety, online		
Q27	**Who is responsible to protect personal data on line?**	
2701	On the Internet, it is my responsibility to protect my personal data	1
2702	It is the government responsibility to protect my personal data online	2
2703	It is everybody's responsibility to make sure personal data are safe online	3
2704	It is the responsibility of the company I transact with to protect my personal data online	4
2705	It is the responsibility of the police and courts to ensure that personal data are protected online	5

Identity behaviour					
Q28	**On Internet, how often do you …**	Never	Sometimes	Often	Always
2801	Give your real identity	1	2	3	4
2802	Use a pseudonym	1	2	3	4
2803	Give a minimum of information	1	2	3	4
2804	Give wrong information	1	2	3	4
2805	Do not answer personal questions	1	2	3	4
2806	Give the identity of another person	1	2	3	4

Behavioural self-protection measures					
Q29	**On the Internet, I usually protect my personal data and identity in the following ways**	Never	Sometimes	Often	Always
2901	Read the privacy policy of web sites	1	2	3	4
2902	Use dummy email account to shield my identity	1	2	3	4
2903	Update virus protection	1	2	3	4
2904	Scan data with anti-spy ware	1	2	3	4
2905	Install operating system patches	1	2	3	4
2906	Erase cookies	1	2	3	4
2907	Use tools and strategies to limit unwanted email (spam)	1	2	3	4
2908	Check that the transaction is protected or the site has a safety badge before I enter valuable personal data	1	2	3	4
2909	Adapt my personal data so that no linking between profiles is possible	1	2	3	4
2910	Change the security settings of my browser to increase privacy	1	2	3	4
2911	Use tools limiting the collection of personal data from my computer (e.g. Firewall, cookie filtering)	1	2	3	4

5. Knowledge of Laws and Protection Systems

Rights (in general)					
Q30	**Do you know your rights in terms of data protection?**	I never heard about it	I heard about it but I do not know it really	I know a little bit about it	I know it very well
3001		1	2	3	4

Perceived protection				
Q31	**For each of the following statements, please state if you tend to agree or not**	Strongly disagree	To	Strongly agree
3101	In [country], my personal data are properly protected	1		7
3102	[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	1		7
3103	I believe that the systems used by the public authorities to manage the citizens' personal data are technically secure.	1		7
3104	I believe that citizens will be able to keep a good level of control over their personal data	1		7
3105	I will always be able to rely on public authorities for help if problems arise with my personal data	1		7
3106	I believe that the authorities that manage my personal data are professional and competent	1		7

Desirable protection				
Q32	**What do you think are efficient ways to protect your identity, online and offline?**	Very efficient	To	Not at all efficient
3201	Give users more direct control on their own identity data	1		4
3202	Allocate more resources to monitoring and enforcing existing regulations	1		4
3203	Require that service providers take greater care of their customer's identity	1		4
3204	Find better technical solution that preserve users' privacy and safety	1		4
3205	Provide formal education on safe identity management	1		4
3206	Raise awareness of the implication of unsafe identity behaviour	1		4
3207	Set up clear guidelines for safe identity management, online and offline	1		4
3208	Make greater use of warnings and signs to signal possible unsafe behaviours	1		4

6. Individual Variables

Gender			
Q33		Male	Female
3301	You are:	1	2

Age			
Q34			
3401	Your year of birth		

Professional situation		
Q35	**What is your actual professional situation?**	
3501	Student	1
3502	Self-employed	2
3503	Manager	3
3504	Other white collar	4
3505	Blue collar	5
3506	Homemaker	6
3507	Unemployed	7
3508	Military/civil service	8
3509	Other	9
3510	Specify	10

Professional situation of head of household		
Q36	**What is the professional situation of the head of your parents' household?**	
3601	Self-employed	1
3602	Manager	2
3603	Other white collar	3
3604	Blue collar	4
3605	Homemaker	5
3606	Unemployed	6
3607	Retired	7
3608	Other	8
3609	Specify	9

Education		
Q37	**What was your full time last year education level? (to adapt to each country)**	
3701	Phd	1
3702	MA, msc	2
3793	Postgraduate certificate, diploma	3
3704	BA, bsc	4
3705	Graduate certificate, diploma	5
3706	Professional qualification	6
3707	HNC, HND	7
3708	A2	8
3709	AS	9
3710	GCSE	10
3711	Year 11	11
3712	Other	12
3713	Specify	13

Urban/rural zone				
Q38		A metropolitan zone	Other urban zone	A rural zone
3801	You live in…	1	2	3

Thank you for your participation!

6. Appendix 2: Further Tables and Figures

Table 40 Profile of completed vs. partly completed submissions

		Full response	Part response	Total
Country	France	**38%**	36%	37%
	UK	**24%**	20%	22%
	Spain	22%	**31%**	27%
	Germany	**16%**	13%	14%
How long have you been using the internet	Less than 1 year	2%	**4%**	3%
	Between 1 and 3 years	12%	**16%**	15%
	Between 3 and 5 years	19%	19%	19%
	More than 5 years	**66%**	60%	63%
Connection frequency	Several times a day	2%	**4%**	3%
	Once a day	12%	**16%**	15%
	Less than once a day	**86%**	79%	82%
Internet trust level	Low	39%	43%	39%
	Medium	28%	26%	27%
	High	34%	31%	33%
Informational privacy concerns	Very concerned	24%	26%	24%
	Somewhat concerned	35%	31%	35%
	Neither concerned nor unconcerned	30%	32%	30%
	Unconcerned	11%	11%	11%
Identity concerns	Very concerned	19%	**24%**	19%
	Somewhat concerned	**47%**	40%	46%
	Neither concerned nor unconcerned	28%	**29%**	28%
	Unconcerned	7%	**7%**	7%
Innovativeness	Low	23%	**30%**	27%
	Medium	**43%**	39%	41%
	High	**35%**	31%	33%
Scenario number	1	24%	**25%**	24%
	2	**27%**	22%	25%
	3	25%	**25%**	25%
	4	24%	**28%**	26%
Check email	No	1%	**3%**	2%
	Yes	**99%**	97%	98%
Would you recommend that your friend subscribes to the service?	Strongly recommend	8%	**10%**	9%
	2	**20%**	19%	19%
	3	**42%**	41%	42%
	4	**18%**	16%	17%
	Strongly discourage	12%	**14%**	13%

		Full response	Part response	Total
If privacy is fully preserved	Yes	**93%**	91%	92%
	No	7%	**9%**	8%
The central government	No	66%	**69%**	67%
	Yes	**34%**	31%	33%
I would trust the system	Strongly disagree	20%	**22%**	21%
	2	**16%**	14%	16%
	3	**19%**	18%	19%
	4	**22%**	21%	22%
	5	11%	11%	11%
	6	6%	5%	6%
	Strongly agree	6%	9%	7%
Electronic signature	Never heard	11%	13%	11%
	Cannot explain	**37%**	33%	36%
	Can explain	52%	**54%**	52%
Usually give online Postal address	Yes	**66%**	61%	65%
	No	31%	**34%**	31%
	Don't know	3%	**6%**	4%
To make a good action, to help	Very likely	**14%**	13%	14%
	2	**34%**	32%	34%
	3	32%	32%	32%
	4	**13%**	11%	12%
	Very unlikely	8%	**12%**	8%
Give a minimum of information	Never	4%	**8%**	5%
	2	36%	36%	36%
	3	**42%**	34%	41%
	Always	18%	**23%**	19%
Attitude toward adopting the eID system	Good idea	39%	36%	38%
	Not good nor bad	33%	36%	35%
	Bad idea	28%	28%	28%

Table 41 internet activities per country

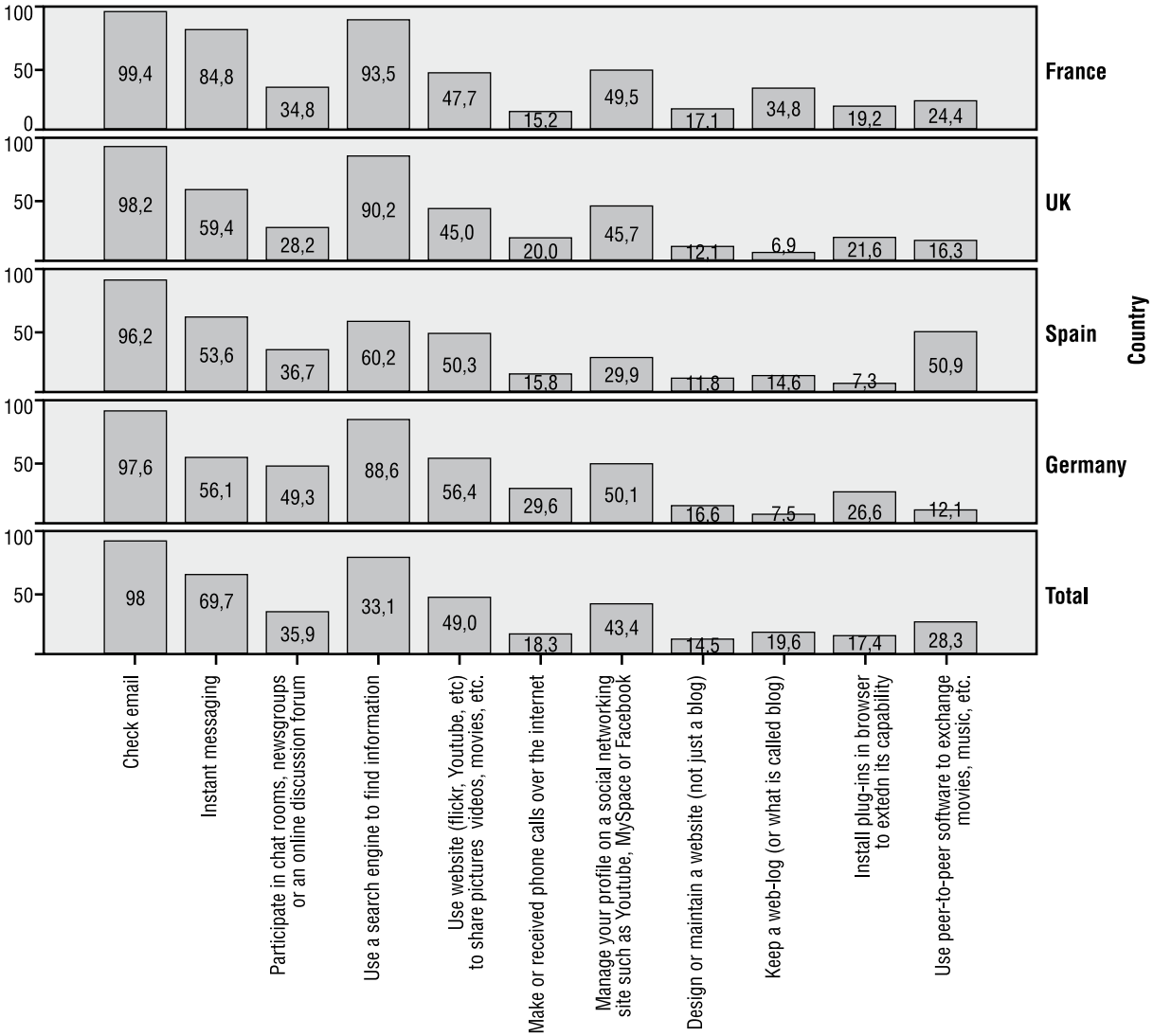


Table 42 Profiles of people who belong to clusters on 'Internet activities'

		Internet activities clusters			Total
		1	2	3	
Country	France	35%	**62%**	29%	38%
	UK	**24%**	10%	**24%**	21%
	Spain	**29%**	20%	**29%**	27%
	Germany	12%	9%	**18%**	14%
Sex	Male	**58%**	53%	56%	56%
	Female	42%	47%	44%	44%
Age	15-18	**55%**	51%	47%	51%
	19-21	19%	**23%**	21%	20%
	22-25	26%	26%	**32%**	28%
You live in…	Metropolitan zone	25%	23%	**33%**	27%
	Urban zone	45%	**48%**	45%	46%
	Rural zone	**30%**	**30%**	22%	28%
How long have you been using the internet	Less than one year	**4%**	2%	2%	3%
	Between 1 and 3 years	**16%**	12%	13%	14%
	Between 3 and 5 years	20%	20%	19%	20%
	More than 5 years	60%	**66%**	**65%**	63%
Connection frequency	Several times a day	**4%**	2%	2%	3%
	Once a day	**16%**	12%	13%	14%
	Less than once a day	80%	**86%**	**84%**	83%

Table 43 Profile of people with low, medium and high innovativeness

		Innovativeness			Total
		Low	Medium	High	
Country	France	35%	40%	39%	38%
	UK	24%	21%	20%	21%
	Spain	23%	28%	29%	27%
	Germany	18%	12%	11%	13%
Sex	Male	44%	53%	70%	56%
	Female	57%	48%	30%	44%
Age ***	15-18	52%	52%	49%	51%
	19	21%	20%	21%	20%
	22-25	27%	28%	30%	28%
You live in… ***	Metropolitan zone	27%	27%	26%	27%
	Urban zone	46%	45%	46%	46%
	Rural zone	28%	28%	28%	28%
How long have you been using the internet	Less than 1 year	4%	3%	2%	3%
	Between 1 and 3 years	20%	14%	10%	14%
	Between 3 and 5 years	23%	21%	15%	20%
	More than 5 years	53%	63%	73%	63%
Connection frequency	Several times a day	4%	3%	2%	3%
	Once a day	20%	14%	10%	14%
	Less than once a day	76%	83%	88%	83%

NOTE: *** Differences reported not significant at $p < 0.01$

Table 44 Cluster analysis of elements encouraging the use of eID systems

	Clusters		
	No	**All**	**Peer trust**
A receipt after you have provided the information	0	1	1
Information on the identification system	0	1	1
Information on the use of the data you provide	0	1	1
Testimonials of persons having experimented the identification system	0	1	0
The assurance that law on personal data protection is respected	0	1	1
A label or logo proving that the system is secure	0	1	1
Guarantees that data are not resold or reused by another organization	0	1	1
A single record with all my transactions, interactions, traces	0	1	1

Table 45 Profiles of people who belongs to clusters on 'preferred eID enablers'

		Clusters on 'eID preferred enablers'			Total
		Guarantees	**Control**	**Peer trust**	
Country	France	30%	**43%**	**44%**	40%
	UK	**24%**	20%	**25%**	23%
	Spain	**27%**	20%	23%	23%
	Germany	**19%**	16%	9%	15%
Sex	Male	**59%**	52%	**59%**	56%
	Female	41%	**48%**	42%	44%
Age	15-18	50%	50%	53%	51%
	19-21ans	20%	21%	21%	20%
	22-25	30%	29%	26%	28%
You live in…	Metropolitan zone	30%	25%	26%	27%
	Urban zone	42%	46%	47%	46%
	Rural zone	28%	29%	27%	28%
How long have you been using the internet	Less than 1 year	**3%**	2%	2%	2%
	Between 1 and 3 years	**16%**	13%	10%	13%
	Between 3 and 5 years	**21%**	21%	17%	20%
	More than 5 years	60%	65%	**71%**	65%
Connection frequency	Several times a day	**3%**	2%	2%	2%
	Once a day	**16%**	13%	10%	13%
	Less than once a day	81%	**85%**	**88%**	85%
Internet trust level	Low	**44%**	37%	39%	39%
	Medium	**29%**	27%	26%	27%
	High	28%	**36%**	**36%**	33%
Identity concerns	Very concerned	24%	**26%**	22%	24%
	Somewhat concerned	28%	**38%**	**38%**	35%
	Neither concerned nor unconcerned	**36%**	27%	29%	30%
	Unconcerned	**12%**	10%	11%	11%
Informational privacy concerns	Very concerned	**21%**	18%	19%	19%
	Somewhat concerned	35%	**51%**	**51%**	46%
	Neither concerned nor unconcerned	**34%**	25%	25%	28%
	Unconcerned	**10%**	6%	5%	7%
Innovativeness level	Low	**30%**	21%	21%	24%
	Medium	41%	42%	**43%**	42%
	High	29%	**37%**	**36%**	34%
NOTE: *** Differences reported not significant at p < 0.01					

Table 46 Factor analysis of opinions on rights of data protection

	Factor Loadings
[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	0.84
I believe that the authorities that manage my personal data are professional and competent	0.82
[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	0.80
I will always be able to rely on public authorities for help if problems arise with my personal data	0.79
In [country], my personal data are properly protected	0.78
I believe that citizens will be able to keep a good level of control over their personal data	0.70

Table 47 Levels of trust in different agents' handling of personal data by country

	% of very or somewhat trust				
	Total	France	UK	Spain	Germany
A friend, a member of family	87	93	82	82	88
The local council	27	40	29	29	40
The national government	32	31	27	27	34
The European Union	32	32	24	24	32
A well-known company	34	32	41	41	27
A company I am familiar with	48	50	47	47	52
An unknown company	4	2	4	4	7
A non-profit association	20	21	17	17	25

Table 48 Cluster analysis of opinions on rights of data protection

	Clusters		
	1	2	3
In [country], my personal data are properly protected	4	6	2
[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	4	5	2
[Nationality] legislation can cope with the growing number of people leaving personal information on the Internet	4	5	2
I believe that citizens will be able to keep a good level of control over their personal data	3	5	2
I will always be able to rely on public authorities for help if problems arise with my personal data	3	5	2
I believe that the authorities that manage my personal data are professional and competent	4	5	2

Table 49 Profiles of people in clusters on 'preferred data protection measures'

		Clusters on preferred Data protection measures				Total
		1	2	3	4	
Country	France	**41%**	33%	39%	**42%**	39%
	UK	21%	**29%**	19%	**26%**	24%
	Spain	**24%**	22%	**26%**	16%	22%
	Germany	14%	**16%**	15%	**16%**	15%
Sex	Male	49%	**66%**	51%	**62%**	56%
	Female	**51%**	35%	**49%**	38%	44%
Age ***	15-18	**54%**	**52%**	50%	49%	51%
	19	20%	18%	**22%**	**22%**	20%
	22-25	27%	**30%**	28%	**29%**	28%
Residence ***	Metropolitan zone	26%	26%	**28%**	26%	27%
	Urban zone	**48%**	**46%**	42%	46%	46%
	Rural zone	26%	28%	**30%**	**28%**	28%
How long have you been using the internet	Less than 1 year	2%	1%	**4%**	2%	2%
	Between 1 and 3 years	12%	10%	**16%**	12%	12%
	Between 3 and 5 years	**21%**	16%	**22%**	19%	20%
	More than 5 years	65%	**74%**	59%	**68%**	66%
Connection recod2	Several times a day	2%	1%	**4%**	2%	2%
	Once a day	12%	10%	**16%**	12%	12%
	Less than once a day	86%	**89%**	81%	**87%**	86%
Internet trust level	Low	37%	**39%**	**42%**	39%	39%
	Medium	27%	26%	**31%**	26%	27%
	High	**37%**	**35%**	28%	**35%**	34%
Informational privacy concerns	Very concerned	25%	**33%**	19%	19%	24%
	Somewhat concerned	**40%**	36%	32%	31%	35%
	Neither concerned nor unconcerned	26%	22%	**37%**	**36%**	30%
	Unconcerned	9%	9%	**11%**	**15%**	11%
Identity concerns	Very concerned	17%	**29%**	15%	15%	19%
	Somewhat concerned	**54%**	**49%**	40%	43%	47%
	Neither concerned nor unconcerned	25%	17%	**37%**	**31%**	28%
	Unconcerned	4%	5%	**8%**	**11%**	7%

NOTE: *** Differences reported not significant at $p < 0.01$

Table 50 Cluster analysis of personal data management strategies

	Clusters	
	1	2
Give your real identity	**3**	2
Use a pseudonym	2	**3**
Give a minimum of information	2	**3**
Give wrong information	1	2
Do not answer personal questions	2	**3**
Give the identity of another person	1	1

Table 51 Profiles of people in clusters on personal data management strategies

		Identity behaviour		Total
		1	2	
Country	France	21%	**52%**	39%
	UK	**41%**	11%	24%
	Spain	**24%**	21%	22%
	Germany	14%	**16%**	15%
Sex	Male	**59%**	55%	56%
	Female	41%	**46%**	44%
Age	15-18	47%	**55%**	51%
	19-21	20%	**21%**	20%
	22-25	**34%**	24%	28%
You live in…	Metropolitan zone	**32%**	24%	27%
	Urban zone	41%	**48%**	46%
	Rural zone	27%	**28%**	28%
How long have you been using the internet ***	Less than 1 year	**3%**	2%	2%
	Between 1 and 3 years	12%	13%	12%
	Between 3 and 5 years	19%	20%	19%
	More than 5 years	67%	65%	66%
Connection frequency ***	Several times a day	3%	2%	2%
	Once a day	12%	13%	12%
	Less than once a day	86%	85%	86%
Internet trust level ***	Low	40%	39%	39%
	Medium	27%	28%	27%
	High	33%	34%	33%
Identity concerns ***	Very concerned	24%	24%	24%
	Somewhat concerned	34%	35%	35%
	Neither concerned nor unconcerned	31%	29%	30%
	Unconcerned	11%	11%	11%
Informational privacy concerns	Very concerned	**21%**	18%	19%
	Somewhat concerned	44%	**48%**	46%
	Neither concerned nor unconcerned	**28%**	28%	28%
	Unconcerned	7%	7%	7%

NOTE: *** Differences reported not significant at $p < 0.01$

Table 52 Alternative factor analysis of personal data disclosure after recoding

	Factors			
	Low disclosure	**Advanced SNS**	**High disclosure**	**Basic SNS**
Judicial information (criminal record, …)	0.79			
Biometric information (fingerprint, iris…)	0.76			
Medical information (social security number, …)	0.75			
Financial information (revenues, credits, …)	0.68			
ID number	0.45			
Bank information (bank card number, account number, …)	0.44			
Things I do		0.67		
Bodily appearance		0.67		
Tastes / Opinions		0.62		
People I meet regularly, friends, Memberships		0.54		
Places where I usually go		0.51		
Name / surname			0.73	
Age			0.68	
Postal address			0.67	
Nationality			0.56	
Information you give on social networks such as Facebook				0.69
Photos of me				0.66

Table 53 Cluster analysis on information provided on Internet

	Clusters	
	General	**SNS**
Name / surname	1	1
Age	1	1
Nationality	1	1
ID number	2	2
Postal address	1	1
Bodily appearance	**2**	**1**
Things I do	**2**	**1**
Tastes / Opinions	**2**	**1**
People I meet regularly, my friends / Membership of associations	**2**	**1**
Places where I usually go	2	2
Information you give on social networks such as Facebook or Study VZ	**2**	**1**
Photos of me	**2**	**1**
Financial information (revenues, credits, …)	2	2
Medical information (social security number, …)	2	2
Bank information (bank card number, account number, …)	2	2
Judicial information (criminal record, …)	2	2
Biometric information (fingerprint, iris…)	2	2

Table 54 Cluster analysis of information provision

		Clusters on 'information provision'		Total
		General	SNS	
Country	France	37%	**41%**	40%
	UK	**26%**	20%	23%
	Spain	**25%**	22%	23%
	Germany	11%	**17%**	15%
Sex	Male	**59%**	54%	56%
	Female	41%	**46%**	44%
Age	15-18	51%	51%	51%
	19	20%	21%	20%
	22-25	29%	28%	28%
You live in…	Metropolitan zone	24%	**29%**	27%
	Urban zone	44%	**47%**	46%
	Rural zone	**33%**	24%	28%
How long have you been using the internet	Less than 1 year	**3%**	2%	2%
	Between 1 and 3 years	**14%**	12%	13%
	Between 3 and 5 years	19%	**21%**	20%
	More than 5 years	65%	**66%**	65%
Connection frequency	Several times a day	**3%**	2%	2%
	Once a day	**14%**	12%	13%
	Less than once a day	83%	**86%**	85%
Internet trust level	Low	**46%**	34%	39%
	Medium	27%	**28%**	27%
	High	27%	**38%**	33%
Identity concerns	Very concerned	**26%**	23%	24%
	Somewhat concerned	34%	**35%**	35%
	Neither concerned nor unconcerned	**31%**	30%	30%
	Unconcerned	10%	**12%**	11%
Informational privacy concerns	Very concerned	**22%**	17%	19%
	Somewhat concerned	45%	**47%**	46%
	Neither concerned nor unconcerned	27%	**28%**	28%
	Unconcerned	6%	**8%**	7%

NOTE: *** Differences reported not significant at $p < 0.01$

Table 55 Cluster analysis of perceived public protection

		Clusters on 'perceived public protection'			Total
		1	2	3	
Country	France	**42%**	**45%**	26%	39%
	UK	21%	17%	**34%**	24%
	Spain	20%	21%	**27%**	22%
	Germany	**17%**	**17%**	13%	15%
Sex	Male	51%	**57%**	**66%**	56%
	Female	**49%**	43%	34%	44%
Age	15-18	**52%**	**52%**	49%	51%
	19-21	**21%**	20%	20%	20%
	22-25	26%	28%	**32%**	28%
You live in…	Metropolitan zone	26%	**30%**	25%	27%
	Urban zone	**47%**	**48%**	41%	46%
	Rural zone	27%	23%	**33%**	28%
How long have you been using the internet	Less than 1 year	2%	2%	**3%**	2%
	Between 1 and 3 years	12%	12%	**13%**	12%
	Between 3 and 5 years	**21%**	**21%**	17%	20%
	More than 5 years	65%	65%	**68%**	66%
Connection frequency ***	Several times a day	2%	2%	3%	2%
	Once a day	12%	12%	13%	12%
	Less than once a day	86%	86%	85%	86%
Internet trust level	Low	34%	19%	**64%**	39%
	Medium	**34%**	23%	19%	27%
	High	32%	**58%**	18%	34%
Identity concerns	Very concerned	20%	19%	**35%**	24%
	Somewhat concerned	34%	34%	**37%**	35%
	Neither concerned nor unconcerned	**36%**	28%	21%	30%
	Unconcerned	10%	**18%**	7%	11%
Informational privacy concerns	Very concerned	14%	12%	**34%**	19%
	Somewhat concerned	46%	46%	**48%**	47%
	Neither concerned nor unconcerned	**34%**	**29%**	15%	28%
	Unconcerned	6%	**13%**	5%	7%
Innovativeness level	Low	23%	17%	**30%**	23%
	Medium	**46%**	40%	37%	42%
	High	31%	**43%**	34%	34%

NOTE: *** Differences reported not significant at $p < 0.01$

European Commission

EUR 23765 EN – Joint Research Centre – Institute for Prospective Technological Studies

Title: Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks

Authors: Wainer Lusoli and Caroline Miltgen

Editors: Wainer Lusoli, Ramón Compañó, and Ioannis Maghiros

Luxembourg: Office for Official Publications of the European Communities
2009

EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-11330-7
DOI 10.2791/68925

Abstract

One key aspect that could influence the digital identity policy landscape has hardly been studied: the views of the European citizens, particularly the views of the generation that has grown up with digital devices. This survey seeks to find out more about future user needs and requirements in the area of digital identity, with a view to informing EU policy making.

This survey has a twofold objective: identifying a) young people's perception of the risks that the new eID technologies may pose and b) young people's acceptance levels of these risks, and their general motivation and intent regarding the use of these new technologies. In summary, the survey aims to identify the key factors that should encourage or support the development of actual and potential eID-based services, in the views of young European consumers.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMISSION

LF-NA-23765-EN-C

Publications Office
Publications.europa.eu

ISBN 978-92-79-11330-7