The Policy Maker's Anguish:
regulating personal data behaviour between paradoxes and dilemmas

Ramón Compañó
European Commission - Directorate General Joint Research Centre (JRC)
Institute for Prospective Technological Studies (IPTS)
Ramon.compano@ec.europa.eu

Wainer Lusoli
European Commission - Directorate General Joint Research Centre (JRC)
Visiting Research Fellow, University of Chester
Wainer.lusoli@ec.europa.eu

A paper for the Eighth Workshop on the Economics of Information Security (WEIS 2009),
London, 24-25 June 2009

1. Introduction[1]

Regulators in Europe and elsewhere are paying great attention to identity, privacy and trust in online and converging environments. Understanding and regulating identity in a ubiquitous information environment is seen as one of the major drivers of the future Internet economy (OECD, 2008). Regulation of personal identity data has come to the fore including mapping conducted on digital personhood by the OECD (Rundle et al., 2007); work on human rights and profiling by the Council of Europe (Dinant, Lazaro, Poullet, Lefever, & Rouvroy, 2008) and major studies by the European Commission with regard to self-regulation in the privacy market, electronic identity technical interoperability and enhanced safety for young people (Marcus et al., 2007).

These domains overlap onto an increasingly complex model of regulation of individuals' identity management, online and offline. This model comprises consumer policy, where priorities are set based on the critical assessment of location and service fruition and trust and privacy as prerequisites for the future common digital market (Kuneva, 2008); human rights agenda, in line with the consequences of advanced profiling techniques (Dinant et al., 2008) and with surveillance concerns in relation to information society security (Hammarberg, 2008); online safety policy, especially in relation with younger users (EDPS, 2008) policies concerning the right of access to advanced, interoperable EU services in the sphere of justice (European Commission, 2007); and a set of policies regarding the economic impact of future networks (OECD, 2008). This implies a regulatory infrastructure of identity which, if fully sketched, is way grander than one that to date tackles identity-theft and ensures smooth services fruition across the EU (interoperability).

The paper claims that policy makers struggle to deal with issues concerning electronic identity. This has two main reasons: the apparently irrational and unpredictable behaviour of users when engaging in online interactions involving identity management and a seemingly intractable set of dilemmas. The former problem, verily a set of behavioural paradoxes, is compounded by the lack of multi-country, systematic, comprehensive data on users' attitudes and behaviours: trust, privacy, behavioural intentions and confidence in relation to personal identity data. In addition, debate is mainly limited to the so-called privacy paradox and people's willingness to disclose personal data.

Building on empirical survey evidence from four EU countries, this paper examines the last aspect in detail – citizens' management of identity in a digital environment. We build on data from of a large scale [n = 5,265] online survey of attitudes to electronic identity among young Europeans' [France, Germany, Spain, UK] conducted in August 2008. The survey asked questions about perceptions and acceptance of risks, general motivations, attitudes and behaviours concerning electronic identity.

This paper is unusual as it defies the established practice of hypothesis testing, corroboration or rejection. Rather, data and results follow a logical argument to support the main thrust of the paper that identity-related policy making is hampered by multiple aims, behavioural idiosyncrasies and systemic dilemmas. While this may be seen as less than 'scientific' in traditional hard science milieus (physical security of identity systems), it contributes to articulate a debate that is sometimes overlooked in such circles. In the conclusion, the paper argues for the extension of the identity debate to span policy circles,

[1] We wish to thank David Broster for the title of the paper and Carline Miltgen and Christine Balague for their work on the eID survey. The views expressed in this paper are the authors' and do not necessarily reflect those of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of the following information.

the engineering community and a growing section of multi-disciplinary approaches to identity.

2. Existing work on the privacy paradox

The so-called 'privacy paradox' is one of the central topics in the debate on privacy and identity. The privacy paradox states that users are concerned about privacy but they disclose a significant amount of personal data and take no action to protect themselves. Several studies confirmed the paradox. It has been found in experimental settings, with specific reference to the role of risk as a discriminant predictor of attitudes (positive association) vs. behaviour (no association) (Norberg, Horne, & Horne, 2007). The paradox has been found in relation to social networking behaviours among US college students (Gross & Acquisti, 2005). A study of Dutch students confirms the paradox across a range of possible defensive behaviours such as behavioural measures and common and more advanced privacy enhancing technologies (Oomen & Leenes, 2007). For specific services, such as instant messaging, the relation between privacy concerns and protective action may be stronger. People who remain unprotected do so because of lack of skills (Paine, Reips, Stieger, Joinson, & Buchanan, 2007). Again in relation to social networking, young people were found to adopt copings tactics rather than adapting strategically to the new information environment (Tufekci, 2008). This may be a way of reconciling actual behaviours with attitudes and social desirability. Finally, privacy concerns have a negative effect on information disclosure but a positive effect on protection intention; transaction intention, however, remains unaffected. Furthermore, information sensitivity has a negative effect on information disclosure and transaction intention (Shu & Kanliang, 2009). To summarise, people do disclose online despite privacy risks, but go to some length to mitigate the effects of disclosure, especially in relation to sensitive information.

However, work on the privacy paradox struggles to cast a net wider than a single country (e.g. the Netherlands), a target group (e.g. students), a limited theoretical focus (e.g. the paradox itself). This is in some way understandable; most of the studies reviewed are small scale experiments; official, multi-country data that would help casting a wider net are lacking; work is often uni- rather than multi-disciplinary. To your knowledge, five studies come close to an encompassing definition of possible, relevant variables:

- European Commission's Eurobarometer Flash study on 27 Member States on confidence in the Information Society, with questions on security risk awareness / knowledge, damage and protective behaviours (Gallup, 2009);
- European Commission's Eurobarometer Flash study on 27 Member States with questions in relation to data protection in own country, plus one question on privacy-enhancing technologies and one on internet trust (Gallup, 2008);
- OCLC survey of six countries, focusing on social networking and social media in relation to privacy and trust (Rosa et al., 2008);
- OECD review of safety and security official statistics focussing mainly on security, with limited if no focus on other aspects such as privacy trust and confidence (Schaaper, 2008);
- FIDIS (Future of ID in the Information Society Network of Excellence) web survey in 19 EU countries on perceptions of institution-based trust in the handling of personal data (Backhouse & Halperin, 2007).

3. Methodology[2]

To examine citizens' seemingly irrational behaviour concerning the management of the identity in a digital environment, we build on data from of a large-scale online survey of attitudes to electronic identity among young Europeans' in France, Germany, Spain and UK conducted in August 2008. The survey examines the attitudes and behaviours of young people because they are the next generation of internet users, citizens and consumers; arguably, they also differ from previous generating in their proximity to and confidence with new digital technologies (Buckingham, 2008; Palfrey & Gasser, 2008).

Preliminary research steps included two focus groups in each country on a topic guide consonant with the final questionnaire; a two-day expert workshop to validate the questionnaire; a pre-test conducted with 100 young people in the UK in June 2008. Once the questionnaire was finalised and pre-tested, invitations to the online survey were sent to 531,443 young people in France, UK, Spain and Germany, in July and August 2008. The survey obtained 12,143 responses to the first question and 5,265 responses to the whole questionnaire [which we use for the analysis reported here]. The survey obtained at least 10 respondents per country except in Germany, where the number of completed questionnaires was n = 819. Table 1 reports the details of the recruitment process.

Table 1 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%**

In terms of representativeness,

- Of all respondents (partial and complete), 37% from France French, 27% from Spain, 22% from the UK and 14% from Germany.
- Overall 56% are male and 44% female, this proportion being different in some countries, notably in Spain (78% male) and in the UK (65 % male).
- The majority are 15-18 years old (46%), 29% are between 19 and 21 and 26% are 22 years old or older. There are less 'younger' people from the 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 2.6% in England and 50% in Spain).

[2] More details on the methodology of the study are found in Lusoli, W. & Miltgen, C (2009) *Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks*. W. Lusoli, R. Compañó & I. Maghiros (eds.). JRC Scientific and Technical Reports EUR 23765 EN. Sevilla: EC JRC IPTS.

- Considering education, only 2% have a Doctorate and 18% a Master (less in UK and Germany). The most common degree is 'licence' with 41% (30% in UK and Spain).

Overall, therefore, there is considerable variance in terms of socio-demographic factors 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. Conversely, however, the sample represents very closely the internet access and use of young people 15-25 years olds in the respective countries (data not reported here, please refer to Lusoli & Miltgen, 2009).

The survey asked questions about perceptions and acceptance of risks, general motivations, attitudes and behaviours concerning electronic identity. Dimensional analysis and factor analysis were used to extract latent indicators. Below, we provide a list of indicators and variables relevant to this paper. We report below the overall theme of the question/s, the question formulation, the factor/s extracted via dimensional analysis and other items that are used in the discussion. Question wording, options, level of measurement and values are provided in the Appendix.

1. Enablers of identifications systems
Q21 Which of the following elements could encourage you to use identification systems?
2 factors: guarantees and control devices

2. Online personal data disclosure
Q22 Indicate what information you provide on Internet
4 factors: low disclosure [information that gets rarely disclosed], basic social networking [SNS], advanced SNS and high disclosure

3. Internet confidence
Q24 More generally, concerning the Internet, you would say that…
1 factor: Internet confidence
1 single item used in analysis: self-confidence in ability to protect oneself online

4. Privacy risk perceptions
Q26 How concerned are you about the following risks in relation to your personal information
2 factors: identity damage, data tracking

5. Responsibility
Q27 Who is responsible to protect personal data on line?

6. Data protection strategies
Q28 On the Internet, how often do you …
Q29 On the Internet, I usually protect my personal data in the following ways
5 factors: offline strategies [hardware based], online strategies [software based], shielding strategies, minimisation strategies and avoidance strategies

7. Data protection knowledge
Q30 Do you know your rights in terms of data protection?
1 scale of data protection knowledge

8. Data protection attitudes
Q31 For each of the following statements, please state if you tend to agree or not
1 factor: attitude towards data protection

9. Remedies

Q32 What do you think are efficient ways to protect your identity, online and offline?

2 factors: awareness raising and direct intervention

1 single item used in analysis: given users more control on their personal data

The survey also included standard socio-demographic questions and a range of questions on internet access and use, and knowledge and use of identification systems. The latter are used to argue the point in relation to policy makers' dilemmas, discussed in section 5, and are reported in the Appendix. Socio-demographic questions and other questions included in the survey are not reported for reasons of space and relevance to the argument proposed here.

4. Paradoxes

Overall, survey results are in line with previous findings form the literature, particularly those on young people's perception of technologies and public policies, privacy, trust and enablers. However, results point to a number of unexpected attitudes of young people that appear irrational.

[table 2 about here]

4.1. The privacy paradox

The survey confirms the prevalence of the privacy paradox [Table 2, marked in yellow], whereby young people disclose a range of personal information despite high perception of privacy risks. In general, the public is primarily concerned about loss of privacy that lead to security problems but few everyday activities are considered extremely or very private. Our results confirm as much, as disclosure of 'basic' biographic information is unrelated to privacy concern; on the other hand, there is a very weak negative correlation (Pearson's R2 -.04) between these and disclosure of potentially more sensitive data (medical history, etc). 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. But the need to appear seems to justify disclosure in young people's eyes. Online social networking, for instance, is more about enhanced and increased personal disclosure than about the maintenance of wider social networks (Cachia, 2008; The Economist, 2009).

4.2. The control paradox

People desire full control on their personal data, but avoid the hassle to keep it up to date. People know that there are technology tools to protect them and think they may be efficient, but they do not use them [Table 2, marked in red]. More than 70% of respondents think that there are efficient solutions to identity-related problems online. Technical solutions are favoured, alongside other supply-side solutions. While 73% claim that it is efficient to 'give users more direct control on their own identity data', a minority employs strategies such as data minimisation, avoidance or active management of won personal data. In detail, there is no correlation between shielding and minimisation user practices and the call for more user control; there are weak correlations between data avoidance and hardware-based strategies and the perception that user should have more control; and there are conflicting (positive and negative) correlation between employment of Internet-based tactics and user control perception.

4.3. The responsibility paradox

Overall, young people consider that the responsibility to manage personal data is shared. They do not attribute responsibility for the protection of personal data to governments or police and courts. Most young people believe that it is either their own responsibility to

protect their data online or the responsibility of the companies they are transacting with. They are asking for tools that give them more direct control on their own identity data. But at the same time, they are not confident in their own ability to keep their data protected. Overall, while only 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 [Table 2, marked in blue]. Furthermore, young people tend to neglect trust seals and do not appreciate privacy enhancing tools. Overall, there is a negative correlation between perceived efficacy of user control on their own data and perception of actual measures that would enable this control (such as receipts, information on systems and counter-profiling information).

4.4. The awareness paradox

Data protection (DP) legislation is unknown and unloved [Table 2, marked in green]. Young EU citizens' knowledge level about DP laws is low. Even lower is their appreciation of the current DP framework. Paradoxically, more knowledge only breeds slightly more positive attitudes (Pearson's R2 .07). People knowing a lot or nothing about DP (24%), are significantly different in their attitudes. However, for the majority of the people in the middle (76 % knowing a bit or not much) there is practically no correlation with attitudes. Moreover, more knowledge on DP rights does not to influence the behavioural intention to adopt digital services based on personal data disclosure (weak negative correlation). Finally, there is a strong correlation (.37) of self-efficacy with DP attitudes, but not with knowledge. But it is knowledge that gets people to stay protected (correlation .20), rather than attitudes, positive or negative (no correlation). These findings suggest that personal experience may matter more than understanding of the legal system. 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. Tools such as guarantees (labels and logos) appeal to young people, while they also appreciate tools that may assist control of personal data provided to public or private authorities.

5. Dilemmas

Alongside having to deal with a number of paradoxes, policy-makers also face a number of dilemmas when devising identity-related policies.

5.1. The cultural dilemma

As digital culture and behavioural attitudes vary across Member States, pass-par-tout policies are not available. There are significant differences between countries in terms of digital culture and markets. Countries vary in terms of mode of Internet connection. In France, 95% connect using home broadband, but 40% also connect at school or university and 20% through pay wi-fi network. 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.

In terms of Internet activities, discrepancies appear between countries. Managing profile on social networks is today prevalent (43%), although it is less widespread in Spain (30%). France has a blogging and instant messaging culture; French young people author more blogs (35%) than people in other countries (<15%), 85% of French youngsters use instant messaging (more any other country) youngsters are more skilled in Germany than elsewhere. Fewer youngsters from all countries design a web site or install plug-ins than in Germany (27%).

Internet access and activities are important for personal innovativeness, and, in turn, for the take up and regulation of digital services.

5.2. The market fragmentation dilemma

The digital market that supports and profits from personal data disclosure is significantly fragmented. Young EU citizens are Web experts and connected mainly at home using broadband. They constitute a specific part of the population particularly Internet minded. However, they are not a homogeneous group. There are three distinct groups in terms of activities. A group (48%) of new Internet users doing classical activities (check emails; search engines); a group (34%) of older Internet users also having web 2.0 activities on social networks; a group (18%) using all the social possibilities of the Internet such as keeping a blog and participating in online discussion forums and chats. Young, innovative people who have being going online via broadband several times a day for more than 5 years are leaders in relation to managing their identity online. This behaviour often requires significant online disclosure of personal data, which youngsters are mostly happy to provide

However, young people who engage in most advanced internet behaviour have a more positive attitude concerning the Internet and lesser perceptions of risk. How to cater for these two different publics (lesser skilled, likely to disclose, lacking confidence; more skilled, very likely to disclose, having more confidence) is matter of great complexity. This segmentation is further propelled by cultural and economic differences across EU Member States. Difference in technical skills, cultural appreciations and market maturity may lead to different applications of personal data disclosure across the EU. From a policy maker's point of view, however, governments must strive in offering all citizens equal opportunities and this is more likely the lesser such fragmentation.

5.3. The public / private dilemma

Governments, as active stakeholders to promote digital service take-up suffer from a triple dilemma. First, the survey evaluated the perceived benefits and risks towards personal data disclosure. Contradictory perceptions exist. While systems are not always seen as risky, EU citizens demand more security and privacy, personalization of services and ease of use. People want to be safe online, but they are wary of governments. Young people do not trust governments but expect them to act.

Second, the public hand as one of the largest investors of ICTs would be in a key position to shape and promote the development of innovative services based on data disclosure. But the majority of digital services developed by governments are largely regarded as unattractive by young people, making them useless as platform for wider deployment in other domains like leisure, work or business.

Third, unlike business players, governments have little room for manoeuvre for negotiations. While some people would accept profiling in exchange of commercial benefits or personalized services, similar incentives are very limited for governments. It would be unacceptable, for instance, to award a tax discount only to those citizens submitting the tax declaration online, while asking the payment of full taxes all others submitting it in paper.

6. Conclusion

In their decisions, policy makers need to take into account that citizens do not always behave rationally. The paper highlights a number of behavioural paradoxes that became apparent from an online survey of young people. In spite of these apparently irrational patterns, governments are increasingly under pressure to design a viable framework to enable innovative services to the benefit for their citizens, largely based on personal data disclosure.

From many quarters, based on evidence beyond our own survey, there is a strong call for effective, fair and transparent data protection rules (Gallup, 2008, 2009). In our survey, trust in rules (fair play by service providers) emerged as an important factor in addition to traditional understandings of trust. Indeed, there are multiple enablers of identity disclosure. Guarantees, assurance of data protection law respect and precise information on systems are likely to encourage the adoption of services based on personal data disclosure. Solutions based on these principles need implementing, regulating and enforcing.

For this to happen, there is an urgent need to look at a wider picture. 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. The survey confirmed the privacy paradox. It also showed that behavioural paradoxes concerning data control, responsibility and awareness compound the picture. Any solution tailored to tackle the former needs to factor in system effects in other domains. But this, it was argued, is not the full picture altogether. Policy action faces systemic constraints.

Governments have to struggle with a number of dilemmas that further limit the range of viable policy options. First, governments need to design policies that enhance the public good, in contrast to companies that can follow a market segmentation approach. Second, the EU ICT markets are very different across the Member States. Finally, there is a cultural component to take into account. These may become serious issues, as there are considerable differences in attitudes with respect to the use and perception of digital services within society, our survey shows.

This does not mean they may not be viable solutions. The survey shed some limited light on possible options. An obvious approach to increase trust is to reinforce safety concerning privacy and personal data online through technical improvements of personal data management systems. In parallel to technical improvements, there is a need to monitor usage patterns regarding such systems and to understand perceptions in order to identify ways to enhance the take up. Young users place great value on privacy, data control, and free services, but not at the expense of security of procedural fairness. The traditional security / privacy paradigm still prevalent in policy circles needs 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. Finally, there is a need to harness young people's current practices. Regulation may be inspired by personal data management procedures used in online social networking sites and other 'places' and tools that people visit and use. Further investigation is required to understand user motivations and to identify value-added services that may improve daily life and make it easier, at a minimum cost.

Table 2. Correlations between main variables and indicators

Variables and indicators	Self efficacy	Low disclose	Advanced SNS	High disclose	Basic SNS	Risk: data tracking	Risk: identity damage	DP tactics: offline	DP tactics: online	DP tactics: shield	DP tactics: minimise	DP tactics: avoid	Remedies: awareness	Remedies: intervene	Enabler: guarantee	Enabler: control	Remedies: user control	DP attitudes
Low disclosure	.06	1																
Advanced SNS	.06		1															
High disclosure	.04			1														
Basic SNS	.07				1													
Risk: data tracking	-.17	-.04			-.04	1												
Risk: identity damage	-.11				-.06		1											
DP tactics: offline	.05	-.09				.13		1										
DP tactics: online			-.04	-.11	-.07	.06	.08		1									
DP tactics: shielding		.16	.04	-.19		-.08	-.05			1								
DP tactics: minimisation		-.14		.06		.08					1							
DP tactics: avoidance	-.08	-.12		-.23	-.14		.05					1						
Remedies: awareness				.07		.18	.15	.10	.07	-.15			1					
Remedies: intervention	.05		.06	.07	.04	.16	.06	.08		-.06	.06	-.06		1				
Enabler: guarantees		-.15		.15	.05	.16	.04	.16	-.05	-.21	.15		.14	.14	1			
Enabler: control	.05	.04	.07	.04		.04	.06	.05	.07				.09	.09		1		
Remedies: user control [1 item]	-.04	-.05	-.06			-.12	-.04		-.06			.04	-.10	-.72		-.09	1	
DP knowledge [1 item]						.09	.04	.22	.20			-.05		.05	.10	.06	-.05	1
DP attitudes	.37	0.04	0.06	0.09	0.09	-.22	-.11	.04		-.04	.05	-.08		.06	.06	.04	.07	.07
Colour codes	Responsibility paradox		Privacy paradox		Control paradox		Awareness paradox											

NOTE: All correlations shown are significant at the 0.01 level (2-tailed).

References

Backhouse, J., & Halperin, R. (2007). A Survey on Citizen's trust in ID systems and authorities. *Fidis Journal, 1*(Online). Available from <http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf>.

Buckingham, D. (Ed.). (2008). *Youth, identity, and digital media*. Cambridge, MA: MIT Press.

Cachia, R. (2008). *Social Computing: Study on the Use and Impact of Online Social Networking* (IPTS Exploratory Research on Social Computing EUR 23565 EN). Seville: European Commission JRC. Available from <http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1884>.

Dinant, J.-M., Lazaro, C., Poullet, Y., Lefever, N., & Rouvroy, A. (2008). *Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the consultative committee (T-PD)* (T-PD(2008)01). Strasbourg: Council of Europe, T-PD. Available from <http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Documents/Reports_and_studies_by_Experts/CRID_Profiling_2008_en.pdf>.

EDPS. (2008). *Opinion on the proposed multiannual Community programme on protecting children using the Internet and other communication technologies*. Brussels: EDPS. Available from <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-06-23_Children_Internet_EN.pdf>.

European Commission. (2007). *Communication from the Commission - Towards a European e-Justice Strategy* (COM(2008)329 final). Brussels: European Commission - DG JLS. Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0329:EN:HTML>.

Gallup. (2008). *Data Protection in the European Union - Citizens' Perceptions* (Flash Eurobarometer Series 225). Brussels: EC DG JLS. Available from <http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf>.

Gallup. (2009). *Confidence in Information Society* (Flash Eurobarometer Series 250). Brussels: EC DG INFSO. Available from <forthcoming>.

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

Hammarberg, T. (2008). *Strong data protection rules are needed to prevent the emergence of a surveillance society* (Viewpoint 26 May). Strasbourg: Council of Europe, Commissioner for Human Rights. Available from <http://www.coe.int/t/commissioner/Viewpoints/080526_en.asp>.

Kuneva, M. (2008). *Key Challenges for Consumer Policy in the Digital Age* (Speech 08/347). London, 20 June 2008: Roundtable on Digital Issues. Available from <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/08/347&format=HTML&aged=0&language=EN&guiLanguage=en>.

Lusoli, W., & Miltgen, C. (2009). *Young People and Emerging Digital Services. An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks* (JRC Scientific and Technical Reports EUR 23765 EN). W. Lusoli, R. Compañó & I. Maghiros (Eds.) Sevilla: EC JRC IPTS. Available from <http://ipts.jrc.ec.europa.eu/publications/>.

Marcus, J. S., Carter, K., Robinson, N., Klautzer, L., Marsden, C., Reidenberg, J., et al. (2007). *Comparison of Privacy and Trust Policies in the Area of Electronic Communications*. Bad Honnef: wik-Consult/RAND Europe, CLIP/CRID/GLOCOM. Available from <http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/final_report_29_02_08.pdf>.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

OECD. (2008). *The Seoul declaration for the future of the Internet economy*. Seoul: OECD Ministerial meeting, 18 June 2008. Available from <http://www.oecd.org/site/0,3407,en_21571361_38415463_1_1_1_1_1.html>.

Oomen, I., & Leenes, R. (2007). *Privacy Risk Perceptions and Privacy Protection Strategies.* Paper presented at the Policies and Research in Identity Management: First Ifip Wg 11.6 Working Conference on Policies and Research in Identity Management (Idman'07), Rsm Erasmus University, Rotterdam, the Netherlands, October 11-12, 2007. Available from <http://www.springerlink.com/content/m047306774615186/>.

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536. Available from <http://www.sciencedirect.com/science/article/B6WGR-4MVN15B-1/2/7e3ac443740d6534d14b198349c590d4 >.

Palfrey, J., & Gasser, U. (2008). *Born digital : understanding the first generation of digital natives*. New York: Basic Books.

Rosa, C. D., Cantrell, J., Havens, A., Hawk, J., Jenkins, L., Cellentani, D., et al. (2008). *Sharing, Privacy and Trust in Our Networked World*. Dublin, OH: Online Computer Library Center. Available from <http://www.oclc.org/reports/pdfs/sharing.pdf>.

Rundle, M. C., Blakley, B., Broberg, J., Nadalin, A., Olds, D., Ruddy, M., et al. (2007). *At a Crossroads: "Personhood" and the Digital Identity in the Information Society* (STI Working Paper 2007/7). Paris: OECD. Available from <http://www.olis.oecd.org/olis/2007doc.nsf/ENGDATCORPLOOK/NT00005D0E/$FILE/JT03241547.PDF>.

Schaaper, M. (2008). *Measuring security and trust in the online environment: a view using official data* (DSTI/ICCP/IIS(2007)4/FINAL). Paris: EAS, DSTI, OECD. Available from <http://www.oecd.org/dataoecd/47/18/40009578.pdf>.

Shu, Y., & Kanliang, W. (2009). The influence of information sensitivity compensation on privacy concern and behavioral intention. *ACM SIGMIS Database, 40*(1), 38-51.

The Economist. (2009, Feb 26th 2009). Primates on Facebook: even online, the neocortex is the limit. *The Economist*. Available from <http://www.economist.com/science/displayStory.cfm?story_id=13176775&fsrc=nwlehfree>.

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science Technology and Society, 28*(1), 20-36.

Appendix: Survey questions

[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
2102 Information on the identification system
2103 Information on the use of the data you provide
2104 Testimonials of persons having experimented the identification system
2105 The assurance that law on personal data protection is respected
2106 A label or logo proving that the system is secure
2107 Guarantees that data are not resold or reused by another organization
2108 A single record with all my transactions, interactions, traces, so I know what is around about me
2109 Others (specify)
2110 None

[online personal data disclosure]
Q22 Indicate what information you provide on Internet
Yes No Don't know

2201 Name / surname
2202 Age
2203 Nationality
2204 ID number
2205 Postal address
2206 Bodily appearance
2207 Things I do
2208 Tastes / Opinions
2209 People I meet regularly, my friends / Membership of associations
2210 Places where I usually go
2211 Information you give on social networks such as Facebook or Study VZ
2212 Photos of me
2213 Financial information (revenues, credits, …)
2214 Medical information (social security number, …)
2215 Bank information (bank card number, account number, …)
2216 Judicial information (criminal record, …)
2217 Biometric information (fingerprint, iris…)

[Internet confidence]
Q24 More generally, concerning the Internet, you would say that…
7-point scale, Strongly disagree To Strongly agree

2401 The internet has enough safeguards to make me feel comfortable giving my personal details online
2402 The internet is now a robust and safe environment in which to transact.
2403 The internet provides a trusted environment in which to make transactions for leisure, work and business
2404 The internet is safe enough to preserve my privacy as I carry out business and personal activities
2405 I am confident that I can protect my privacy online

[privacy risk perceptions]

Q26 How concerned are you about the following risks in relation to your personal information
5-point scale, Very concerned To Not at all concerned

2601 Companies possess information about me that I consider private
2602 My personal information is used without my knowledge
2603 My personal data is shared with third parties without my agreement
2604 My behaviour and activities can be monitored online
2605 My online personal data is used to send me commercial offers
2606 My identity is reconstructed using personal data from various sources
2607 My views and behaviours may be misrepresented based on my online personal information
2608 My reputation may be damaged by online personal information
2609 My identity is at risk of theft online
2610 My personal safety may be at risk due to online personal information
2611 I may be victim of financial fraud online

[responsibility]
Q27 Who is responsible to protect personal data on line?
Tick one

2701 On the Internet, it is my responsibility to protect my personal data
2702 It is the government responsibility to protect my personal data online
2703 It is everybody's responsibility to make sure personal data are safe online
2704 It is the responsibility of the company I transact with to protect my personal data online
2705 It is the responsibility of the police and courts to ensure that personal data are protected online

[data protection strategies 1]
Q28 On Internet, how often do you …
Never Sometimes Often Always

2801 Give your real identity
2802 Use a pseudonym
2803 Give a minimum of information
2804 Give wrong information
2805 Do not answer personal questions
2806 Give the identity of another person

[data protection strategies 2]
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
2902 Use dummy email account to shield my identity
2903 Update virus protection
2904 Scan data with anti-spy ware
Q2905 Install operating system patches
2906 Erase cookies
2907 Use tools and strategies to limit unwanted email (spam)
2908 Check that the transaction is protected or the site has a safety badge before I enter personal data
2909 Adapt my personal data so that no linking between profiles is possible

2910 Change the security settings of my browser to increase privacy
2911 Use tools limiting the collection of personal data from my computer (e.g. Firewall, cookie filtering)

[data protection knowledge]
Q30 Do you know your rights in terms of data protection?
Tick one

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

[data protection attitudes]
Q31 For each of the following statements, please state if you tend to agree or not
7-point scale, Strongly disagree To Strongly agree

3101 In [country], my personal data are properly protected
3102 [Nationality] legislation can cope with the growing number of people leaving personal information on the Internet
3103 I believe that the systems used by the public authorities to manage the citizens' personal data are technically secure.
3104 I believe that citizens will be able to keep a good level of control over their personal data
3105 I will always be able to rely on public authorities for help if problems arise with my personal data
3106 I believe that the authorities that manage my personal data are professional and competent

[remedies]
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
3202 Allocate more resources to monitoring and enforcing existing regulations
3203 Require that service providers take greater care of their customer's identity
3204 Find better technical solution that preserve users' privacy and safety
3205 Provide formal education on safe identity management
3206 Raise awareness of the implication of unsafe identity behaviour
3207 Set up clear guidelines for safe identity management, online and offline
3208 Make greater use of warnings and signs to signal possible unsafe behaviours

[Internet access and activities]
Q2 How do you connect to the Internet ?
Tick all that apply

201 Where I usually live (home, parent's home, Uni) using broadband
202 Where I usually live (home, parent's home, Uni) using dial-up
203 At work
204 At school or university
205 Through pay wi-fi network (airport, train station…)
206 In an internet cafe

Q3 How often do you connect to the Internet?

Tick one

301 Several times a day
302 Once a day
303 A few times a week
304 Less than once a week
305 Less than once a month
306 Never

Q4 What devices do you use to connect to the Internet?
Tick all that apply

401 Personal Desktop PC
402 Shared Desktop PC
403 Laptop computer
404 WII, playstation or other gaming console
405 On mobile phone or PDA, using GPRS or 3G

Q5 Do you do the following activities on the internet?
Tick all that apply

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