Public Perception of the Data Environment (*) and Information Transactions

A selected-survey analysis of the European public's views on the data environment and data transactions (**)

Dara HALLINAN & Michael FRIEDEWALD (***)
Fraunhofer Institute for Systems and Innovation Research ISI, Germany

Abstract: When engaging in data transactions, it has consistently been observed that individuals' behaviour does not correspond with individuals' theoretically stated preferences about privacy and the importance of personal data. This paper considers this 'paradox'. First, through an analysis of selected surveys, we elaborate a picture of how the public perceives the data environment and their interaction with it. We find that, whilst the public places significant weight on the values of privacy and data protection and has a formal understanding of the features of the data environment, there is a significant knowledge deficit relating to the specifics of data flows and processing. Although the public felt that they were being forced into engaging in an ever increasing number of data transactions, they lacked the clarity and understanding to evaluate the significance of these transactions either at the individual or social level. We then consider how these findings relate to specific transactions involving personal data transfer. Acquisti and Grossklags theorise that decision making may be unbalanced by limited information, bounded rationality issues, psychological distortions and ideology and personal attitudes. Using the findings from our selected survey analysis, we add substance to these claims. The lack of understanding of the data environment coupled with the necessity to act in this environment accounts for impacts on each limiting factor and reduces the ability for the individual to 'rationally' balance each transaction. Awareness of issues (and the importance allocated to personal data) on an abstract scale does not translate to the apparently corresponding action in concrete situations.

Key words: privacy, trust, personal data, data protection, privacy paradox, public opinion, consumer behaviour.

(*) The data environment describes the totality of data collection and data flows, the physical infrastructures that make this possible and the actors and their goals involved.

(**) Some of the content for this paper is based on HALLINAN, FRIEDEWALD & McCARTHY (2012). This paper represents an expansion of findings in that paper, particularly as they offer insight into the supposed 'privacy paradox' and behaviour in specific transactions.

(***) Acknowledgement: This paper is based on research undertaken in the SAPIENT (Supporting Fundamental Rights, Privacy and Ethics in Surveillance Technologies) project funded under the European Commission's 7th Framework Programme for research and technological development under Grant Agreement no. 261698.

The aim of this paper is firstly to elaborate how the European public perceives the data environment and their place within it on an abstract level, and secondly to apply observations gained to behaviour regarding specific transactions. Accordingly, the article will seek to add clarity as to why individuals behave the way they do when engaging in data transactions – behaviour that at first sight, appears erratic and even contradictory to declared privacy preferences.

'The public' are central to all debates relating to information processing and assumptions as to what 'the public' think are consistently made. However, the reality of the public's opinions on the data environment remains seldom considered. This paper seeks to address this discrepancy.

Whilst this paper draws heavily on public opinion surveys as its base resource, surveys have been supplemented – as the quantity of applicable surveys was limited, as their focus was often narrow and as their results were difficult to extrapolate into more elaborated explanations of opinion and behaviour – by sources employing other methodologies, such as ethnographic studies and focus groups. This mixed methodology approach, the scarcity of data and the complexity and breadth of the subject makes the traditional meta-survey analysis approach (considering the significance of methodological similarities and differences in results and trends) very difficult. Accordingly, and as opposed to other meta-survey analyses, this paper focuses on isolating trends across surveys which can be used to assist in the construction of a picture of the public's conception of the data environment. [1]

After brief comments on certain methodological issues present in such a survey analysis and on the diverse nature of the public under consideration, the main part of the paper is split into two. The first section attempts to paint a broad strokes picture of public perception of the data environment. This section firstly considers the importance the public place on personal data. Then it addresses public understanding and conception of the physical environment, including: actors and their motivations, the links and data flows between actors, the infrastructure of data processing and the potential in data processing. Finally, public interaction with this environment is considered, elaborating what the public fear and believe the dangers are, in interacting with this environment and how they justify their interaction despite

[1] Doing a traditional meta-survey analysis was impractical here, but would be an excellent option for further research.

these fears. In the second part, we apply findings from part one onto thinking regarding specific data transactions. ACQUISTI & GROSSKLAGS (2004, pp. 171-76) suggest certain factors which may be specifically relevant in unbalancing an individual's 'rational' approach to a data transaction. We consider our findings in the light of these factors, demonstrating how flawed conception and lack of understanding of critical parts of the data environment may translate into imbalance in each individual transaction.

■ Problems with surveys and the selected survey methodology considering the data environment

Public opinion is a notoriously difficult substance to judge – not least owing to the nuance and constant shift of individuals' opinions. Public opinion is particularly difficult to judge in relation to complex, value laden and abstract issues such as individuals' conceptions data flows and the data environment (HARPER & SINGLETON, 2001).

In this analysis, certain issues should be specifically borne in mind as problematic. Firstly, surveys are an imprecise tool in the creation of an image of a diverse public. Secondly, with each survey, a number of methodological flaws can influence the reality and truth of eventual findings. [2] Thirdly, considering the abstract nature of the subject matter, it is difficult to gauge whether answers to survey questions genuinely reflect individuals' perceptions related to the question topic or how much they tell us about how strongly convictions indicated in an answer are actually held. In the focus groups sources considered it was evident that many had not spent much time considering the issues in focus and also that, as the discussions went on, opinions could even be seen to change (for example in MURPHY, 2007). Finally, whilst this paper has a broad remit and addresses a number of different areas, surveys have tended to be more limited in scope (even the large scale Eurobarometer surveys). This means that information has been pulled from a range of surveys whose thematic comparability was difficult to gauge.

[2] For example, the biased effect created by the motivations of the key players in the survey process or inherent flaws in survey methodology – such as potential biases created by flawed concept framing or question clarification.

As the section seeks to explore European attitudes, the key surveys have a Europe wide sample population. This unfortunately narrowed the number of useable surveys. When going further into depth in an issue, it was often necessary to use more local and in depth surveys. This poses issues in the extrapolation of general conclusions from local data.

■ There is more than one 'public'

This article seeks to understand how the European public understand and view the data environment and their transactions with that environment. However, it must be pointed out that the European public is a diverse body in which an enormous range of views and perspectives are present. There are a range of factors that can have an effect on perceptions and approaches toward the use of data generally and in specific instances, such as social status, political affiliation, income, education, profession and gender. The correlations of these factors to a stance can be very difficult to pick apart and would also presumably be highly context dependant.

Particularly significant appear to be nationality (and consequently national culture) and age (or more precisely, familiarity with the digital environment). The differences between national results in surveys can be considerable. In Eurobarometer 359 (TNS Opinion & Social, 2011) [3] for example, trust in banks and financial institutions varied from 49% in Romania to 92% in Denmark (whilst these numbers may have changed due to the financial crisis). An expansion of this even reveals broader regional trends – for example, a Scandinavian group perspective can be isolated. In the same survey there is a specific separation and investigation into the specifics of digital natives and initiates (those who were born and raised with, or subsequently became familiar with, digital technology) and other, predominantly older, respondents (ZUREIK *et al*., 2010; BELLMAN *et al*., 2004; SAMATAS, 2005). [4]

[3] See also the extensive analysis of this Eurobarometer survey by LUSOLI *et al*. (2012).

[4] Whilst the authors have not found consistency enough to consider the significance of causal factors at the individual level, this is a potential area for future research.

■ Public perception and comprehension of the data environment

The public and personal data

From survey results it is clear the public allocates data protection and privacy significant importance. Indeed in the 'Public Awareness Survey 2008' carried out on behalf of the Irish Data Protection Commissioner the privacy of personal information was ranked 3rd in order of importance (with 84% regarding it as 'very important') in a list of key issues, trailing crime prevention by only 3% (Landsdowne Market Research, 2008).

Despite the high importance allocated to the protection of data, it is also apparent that a large portion of the public feel that they have lost control of their data (ALLWINGER & SCHILLAB, 2008) and that the data protection systems in place are inadequate for the task. In Flash Eurobarometer 225 a majority of respondents believed that national legislation could not cope with the demands currently placed on it (The Gallup Organization, 2008).

Actors

Surveys generally distinguished between state actors and private organisations. Within this differentiation, state actors tended to be (often considerably) more trusted than private actors. This was broken down further to show that certain state sectors were trusted more than others. In 'Flash Eurobarometer 225' (The Gallup Organization, 2008) medical services were highly trusted with an 82% positive trust rating, whereas local authorities scored a lower 67%. However, these numbers perhaps obscure a nuanced understanding of trust. When the public is further questioned on the issue of trust in state institutions, whilst there seems to be a belief that institutions will try to behave in the right way, there is a far lower belief in their capability to safeguard data. It has been suggested that this could be partly as a result of media coverage given to authorities' leakage of personal data (BACKHOUSE & HALPERIN, 2007).

Within the private sphere there is also considerable trust variation. In the same Eurobarometer survey, banks received a 66% trust rating whilst mail order companies received only 24% (The Gallup Organization, 2008).

However deeper opinion regarding commercial organisations handling of personal data revealed a distinct undercurrent of distrust.

Interestingly, whilst responses predominantly disapproved of sharing between government and private organisations, there was little elaboration as to what the public believed the model of interaction between organisations actually is, or to public perception of balance or substance to the storage or flow of data between organisations. In essence, there was little elaboration of a model beyond the first instance of data collection. It would be logical to suggest that the public have a limited conception of which organisations possess information on them and accordingly, for what purposes this information is being used (BRANDTZAEG & LÜDERS, 2009, pp. 38-56). Consequently, one could argue, without comprehension of various actors' presence, involvement and motives and accordingly their shaping of information flows (and eventually, also personal impact), it is impossible for individuals to build a picture of the operation of the data environment. A keystone for trust, accountability and transparency is thus missing. Equally, it does not seem that large data processing organisations are particularly working to address this. Research suggests, "for the ordinary citizen, entering into contact with [...] 'big' data controllers is nearly impossible" (GELLERT & GUTWIRTH, 2012, p. 42).

Responsibility allocation

When asked directly, the public does not seem certain which actors should be responsible for the safe handling of personal data. Indeed, opinion on who should be responsible changes depending on the nature of the entity, or sector, dealt with. When considering social networking sites for example, 49% of respondents stated the individual should be primarily responsible with 33% suggesting the social network should be responsible, whilst in relation to online shopping sites the percentages were 41% and 39% respectively (TNS Opinion & Social, 2011). The difference is interesting not only as it demonstrates uncertainty in responsibility allocation but also as it suggests a difference in perception based on the nature of the specific data processing entity. Taking this logic one step further suggests the public may be basing an approach more on the entity dealt with as opposed to centred around data and the processing of data. Equally interesting is the relatively low response listing public authorities as having primary responsibility - 16% and 19% respectively (TNS Opinion & Social, 2011).

This allocation is, to some extent in contrast with the relatively harsh penalties (if there is such uncertainty as to who should hold responsibility it seems strange there should be preference for harsh regulation) the public seems to wish penalties? on organisations that breach standards. Indeed, in the same Eurobarometer survey, 51% of respondents suggested organisations which misused data should be fined, with 40% believing such organisations should be banned from using such data (TNS Opinion & Social, 2011).

Impacts and fears

In terms of tangible impact, as a consequence of a release of information and the dangers it entailed, the public seemed specifically concerned about ID fraud, which was perceived to be a serious threat (Landsdowne Market Research, 2008). This concern was relevant to both state and commercial organisations. There was also undefined concern about other forms of physical or material harm. Particularly in the case of ID Fraud, this may have something to do with the amount and tone of media coverage. Murphy points out the perception that "it is very easy for people to de-fraud you and that there is very little you can do to stop it, even if you take precautions" (MURPHY, 2007). The public also demonstrated concern relating to the commercial collection and use of data. Unsurprisingly, the public displayed fears relating to individual impact. They displayed concern and annoyance by the perceived end results of data distribution, namely direct mail, spam, cold calling etc. Related to this, the public showed concern relating to certain data practices linked to this fear – the fear that information would be 'used without knowledge', 'shared with third parties without agreement' and 'that information would be used in different contexts than those in which it was disclosed' (TNS Opinion & Social, 2011).

Although there were abstract fears relating to the combination of data and/or databases, and further issues related to assemblages of data etc., these were at best only loosely defined. Murphy states, "some were able to imagine an extreme scenario where these bodies 'join up' the information they hold, thus, to our respondents' eyes, reducing them to pieces of (impartial) data and robbing them of their individuality" (MURPHY, 2007). However, when listing concerns, a small portion of respondents in Eurobarometer 359 were able to recognise the more solid, individually based, manifestation of these concerns; 12, 11 and 7% respectively recognising the risk of 'reputation damage', 'views and behaviours being

misunderstood' and 'the possibility for discrimination in other areas' (TNS Opinion & Social, 2011).

Justifications and benefits

Despite the above risk recognition and general uncertainty and the fact that 63% of respondents state that disclosing personal information is a big issue for them, individuals appear to accept the fact that they must divulge increasing amounts of information (TNS Opinion & Social, 2011). The overarching reason for this acceptance is the deterministic viewpoint that it is 'simply part of modern life'. On the one hand, there is the perceived obligation to release ever more information. The public feel obliged legally, as required by authorities' increased collection practices, and practically, as a price for involvement in the information environment.

On the other hand the public recognises benefits from the further release of information. These take the form of short term benefits in the form of exchanges for rewards (or service usage) as well as longer term benefits from participation in data exchanges and a presence in data environments - social networking for example (BRANDTZAEG & LÜDERS, 2009).

Uncertainty and inconsistency

It is helpful to consider the 'data/information' (as opposed to the 'real world' aspects – such as actors) aspect of the data environment in two parts; supporting technological infrastructure (and its innate capabilities), and the operation of the network of data connections and flows that constitute its lifeblood. [5]

In each consideration of technology, the public showed a lack of awareness as to the capabilities, uses and privacy impacting features. This is demonstrated in the U.S. survey, 'Technology, Security and Individual Privacy: New Tools, Threats and New Public Perceptions' (STRICKLAND &

[5] By 'supporting technological infrastructure' we refer to the technology involved in allowing data flows to exist (much as roads and railways allow the movement of people and goods). This includes computers and software for example. By 'networks of data flows and connections' we refer to the data flowing through this infrastructure and to and from whom this data is flowing (much as vehicles, cargoes and their frequency constitute the 'life blood' of a road infrastructure).

HUNT, 2005). Of a sample of educated citizens regarding various 'novel' information collection technologies it was found that:

> "Certainly, there is not a substantive understanding of the technology [...] Indeed, the high error rate on some of the questions indicates that the subjects clearly underestimate the extent of the technology" (STRICKLAND & HUNT, 2005).

This conclusion is backed up by work done as part of our research into the level of comprehension and acceptance of information gathering technologies. Indeed, we found that the public has little solid understanding of many new technologies or their operation and accordingly that, the critical features and impacts at each individual and social level are subject to uncertainties... [and perception may be] significantly distorted (GUTWIRTH *et al*., 2012).

A lack of understanding as to the shape and operation of the data flows themselves, the capabilities they offer and the software infrastructure behind them is demonstrated by BRANDTZAEG & LÜDERS (2009). They point out that, even within the confines of a single social network, users are neither aware of (amongst a variety of other issues) the intelligent tracking technologies in operation, the connections to different applications or the dynamism of the networks they are taking part in.

From this gap in understanding, it is possible to assume that there are a series of other relevant questions which the public may not yet have the reference points to answer solidly, for example, what the value of their data might be, who might want this data or what the exact social or personal consequences of each release might be (ALLWINGER & SCHILLAB, 2008). Thus, the deterministic approach to obligatory information disclosure can arguably also be seen as a practical coping mechanism. The necessity to act in an environment which the individual does not understand, and in which there is an awareness of risk, still needs justification in the individual's mind.

The broader consequences of this are, firstly, that the public are unable to formulate considered responses and to evaluate their own actions or to build a practical model for behaviour, even to issues they have clearly identified, as they only have half of the relevant foundations through which to do this. Secondly, although the public may be aware of a series of other threats, they are unable to consider responses to them. In this respect, the tangible impacts which are not obviously related to original data collection are ignored, and, as the data processing itself is invisible and the processes

largely not understood, the increasingly broad impact data processing has on a structural level and on other systems (social and economic) is correspondingly invisible.

■ Translation into individual data transactions

Figures can be put on certain aspects of opinion in individual surveys indicating the public place high importance on their personal data and that they are aware of risks in releasing this data. However, there is a considerable difference between actual behaviour and what individuals declare about their privacy in theory. For example with respect to the declared importance of privacy in online environments and behaviour in relation to privacy protection (SPIEKERMANN & GROSSKLAGS, 2005).

In this section we now consider how individuals evaluate specific data transactions, and how the conclusions drawn from the analysis of public perceptions of the data environment on a more abstract level, could shed light onto the more specific context of individual transactions. We thus seek to add clarity to the confusing and contradictory behaviour exhibited by consumers in data transactions.

A helpful contribution encountered in this regard is ACQUISTI & GROSSKLAGS (2004). The authors focus on the economic considerations likely to affect choice and action, and why these may be significant in analysing why individuals' information security attitudes and behaviour may be inconsistent with one another. In this work they consider the possibility that privacy in theory may mean many different things in practice and consequently that "the parameters affecting the decision process of the individual are perceived differently at the forecasting (survey) and operative (behaviour) phases". Along with a number of other interesting observations about individuals' privacy preferences and actual behaviour, they isolate a series of potential limiting factors to the ability of the individual to rationally evaluate a data transaction. They theorise that decision making models may be unbalanced by limited information, bounded rationality issues, psychological distortions and ideology and personal attitudes. [6]

[6] These factors are the most relevant to current analysis. ACQUISTI & GROSSKLAGS also list market behaviour as a potential distortion factor.

This conception of the individual's evaluation of personal data release challenges the traditional concept of privacy economics. In traditional privacy economics, the individual is viewed as a rational, fully informed agent – and therefore an agent fully aware of their actions and the significance of those actions. This conception of the rational individual agent – and by proxy the public as a collection of rational individual agents – has had significant implications for the development of interactions in information environments, for the conception of how actors should behave and how 'trust' should be built within these environments. Accordingly, insight into the causes and mechanics of the discrepancy between declared preferences and actual behaviour offers insight with implications not only for the comprehension of consumer behaviour, but also has normative implications for the behaviour of other actors within, and all policy processes concerning, this environment.

ACQUISTI & GROSSKLAGS (2005) tested these theories with some considerable success, highlighting a number of instances in which declared preferences did not match behaviour and demonstrating the presence of each of the theorised limiting factors to 'rational' decision making. Our analysis retains their theoretical proposition, while approaching the issue from a different perspective. Firstly, Acquisi and Grossklags took a sample of the US public to test their theories. In this investigation, we focus on the EU public. Secondly, their experimentation was designed to test their hypotheses specifically in relation to individual preferences and action – for which they took a small sample and subjected them to considerable targeted questioning and observation. We draw on a much broader approach whose initial goal was to neutrally (in the sense that we did not set out to prove or disprove any hypothesis) construct a picture of the public conception of the information environment. Accordingly our base unit (the public, rather than the individual) as well as our approach, and data set, are considerably different.

Overall, Acquisti and Grossklags theorising appears to fit well with our findings in part one. The perception of the data environment mentioned above would certainly account for impacts on each of these potentially limiting factors and would thus reduce the ability for the individual to 'rationally' balance each action (ACQUISTI & GROSSKLAGS, 2004; SCHÜTZ & FRIEDEWALD, 2011). Consequently, awareness of issues (and the importance allocated to personal data) and what can be done etc. on an abstract scale may not translate to the apparently corresponding action in concrete situations.

In terms of limited information, Acquisti and Grossklags suggest that four features are significant in precluding transactional 'rationality'. Firstly, externalities:

> "When third parties share personal information about an individual, they might affect that individual without his being part of the transaction between those parties".

Secondly, information asymmetries:

> "Information relevant to the privacy decision process might be known only to a subset of the parties making decisions".

Thirdly, due to risk:

> "Most privacy related payoffs are not deterministic".

Finally, due to uncertainties:

> "Payoffs might not only be stochastic, but dependent on unknown random distributions" (ACQUISTI & GROSSKLAGS, 2005).

The confirmation that decision making may be rationally unbalanced by limited information comes through particularly strongly in our findings. The first two features are particularly strongly represented. Our research firstly points strongly to the fact that the public have very little conception of how information is dealt with after an initial release. This indicates that they are not aware of the institutional connections which define the third parties who may come into possession of information. Accordingly they cannot be aware of what those parties may wish to do with the information. Thus, they are unaware of significant externalities which may arise from any transaction and which may have an impact on them. As a consequence of this, in each transaction, the public are vulnerable to significant information asymmetries. These asymmetries are amplified though our observation of a significant lack of technical or systemic understanding of the data environment and accordingly our observation that the public may have had significant difficulty in answering a series of other, more abstract questions – for example relating to the worth/value? of their data. This would certainly create an imbalance in the ability to act rationally, as well as an attendant information asymmetry, considering that the value and use of the data is defined by the processing capabilities of the software and the networks through which it flows. These observations are tightly tied to perception of risk. Firstly, it was clear that the public only had limited concepts of the risks implicit in a data transaction and indeed often overlooked or were unaware of the more abstract risks, simply as they were unable to construct a model to solidify

these risks. Secondly, even when risks were apparent, the public lacked the links and knowledge to specifically quantify these risks in relation to their own actions.

In terms of bounded rationality, Acquisti and Grossklags suggest that:

> "Even if individuals had access to complete information, they would be unable to process and act optimally on vast amounts of data. Especially in the presence of ramified consequences associated with the protection or release of personal information. [Thus] our innate bounded rationality limits our ability to acquire, memorize and process all relevant information, and it makes us rely on simplified mental models, approximate strategies and heuristics" (ACQUISTI & GROSSKLAGS, 2005).

Whilst the consideration of bounded rationality is difficult given the underlying prevalence of incomplete information, we can make some comments on the intentional, and perhaps necessary, simplification of behaviour models. Firstly, it was observable in our research that the public were aware of their own 'rational ignorance' in information transactions, which was viewed as a coping strategy in light of the awareness of risks of information disclosure but the feeling that release of information was often obligatory and becoming more so. This is a fascinating observation and indeed introduces a novel factor into Acquisti and Grossklags' consideration. Consideration of choice in transactions as being 'irrationally' skewed by a series of internal and external factors has tended to focus narrowly on these factors. There is accordingly an underlying assumption that the element of 'choice' itself remains a neutral quantity that does not require further investigation. This is possibly as focus was narrowly focussed on causation between skewing factors and individuals in specific transactions, offering a narrow frame for observation. Our research indicates that the public do not necessarily perceive choice as a neutral quantity and indeed they feel they are being forced to engage in information transactions and to maintain a presence in the information environment. Whilst we do not suggest that the element of choice has been removed from all transactions, we would like to suggest that a context in which the public feel a general necessity to engage in the data environment as part of everyday life has a consequent effect on the mentality and context in which each specific decision is made. This is an observation that may have significant impact on the other skewing factors under consideration and indeed deserves significant further research. Secondly, whilst the public's views seemed occasionally somewhat superficial, it was interesting to observe that, in deeper discussions, individuals would change their perceptions and become aware of

unconsidered risks and contradictions inherent in their own thinking. This indicates a deliberate construction of simplistic but functional models, or at least a deliberate lack of self-reflexion on one's own approaches, for assessing privacy risks and the release of information.

Thirdly, in relation to psychological distortions, Acquisti and Grossklags point out that:

> "Even if individuals had access to complete information and could successfully calculate optimization strategies [...] they might still deviate from the rational strategy. A vast body of economic and psychological literature has revealed several forms of systematic psychological deviations from rationality that effect individual decision making. For example, [...] motivational limitations and misrepresentations of personal utility [...] individuals often mispredict their own futures or draw inaccurate conclusions from past choices [...] individuals often suffer from self-control problems [and] individuals' behaviour can often also be guided by social preferences and norms" (ACQUISTI & GROSSKLAGS, 2005).

The heading of psychological distortion is difficult to consider in terms of the format of our work (and indeed ACQUISTI & GROSSKLAGS, 2005) suggested that corroboration of these factors with evidence may require the use of experimental tests rather than surveys), However, we can perhaps make some observations. Firstly, our findings that the public justified data transactions on the basis of short term rewards, at the expense of an uncertain and ignored privacy impact certainly mirrors observations under the psychological distortion heading suggesting that individuals tend to preference certain short term rewards over uncertain long term risks and losses. Secondly, we would tentatively suggest that the public's decision making may be rationally imbalanced by the perception of a developing norm/social preference toward the release of data. For example, in our findings we note that, the public feel a general necessity toward releasing data in an ever increasing number of situations, and the feeling that the release of data is 'simply a part of modern life'.

Finally, whilst the above factors speak to individuals being practically more inclined to give away personal data despite abstract awareness of risk, we observe in certain of the more in depth focus groups the importance of a final factor – ideology and personal attitude. The strength of attitudes may tip the scales 'irrationally' the other way, leading to an individual excessively refusing to engage in data transactions despite potential benefit, based on related ideological positions – on personal privacy, for example.

■ Conclusion

It is apparent that the public are generally aware of the existence of the data environment and are aware of its growing significance in relation to everyday life. This is perceived to force increasing interaction with the data environment and increase the necessity to release data. In particular the public are aware of the more solid and visible aspects of this environment. For example, there was an awareness of the actors involved and an awareness of specific potential consequences of the processing of data (for example ID fraud or direct mailing and advertising).

However, when considering the more abstract, invisible and complex aspects of this environment, comprehension dropped drastically. There was little comprehension of the value of data, the nature of the technologies involved or the shape or nature of data flows – that is to say, comprehension of the critical parts of the data environment, was conspicuously absent.

Accordingly, in key areas, the public lack the requisite information on which to build accurate and functional models for behaviour and interaction with this environment and for transacting with personal data. For example, it is impossible to build a conception of cause and effect, when effect is separated from cause as a result of a set of invisible systems.

The lack of understanding of the data environment generally, translates onto the evaluation of each data transaction individually. The holes in comprehension impact on certain key factors in the decision making process to reduce the ability for the individual to 'rationally' balance each action. Thus, whilst abstractly the individual may attach high importance to personal data and be aware of certain risks in releasing this data, this does not transfer onto each specific transaction.

Appendix 1: Comparison list of surveys used

Title	*Year*	*Institution/ Author*	*Sector*	*Sample Universe*	*Sample size*	*Field(s)*	*Form of Survey*
Vertrauen der ÖsterreicherInnen in den Datenschutz	2008	Oeconsult	Economic	Austria	1213	Privacy, personal data protection	Representative sample, face to face and online, multiple choice questions
A Survey on EU Citizens' Trust in ID Systems and Authorities	2006	FIDIS Project, EU project	Academic & political	Survey translated into 8 European languages	1906	ID systems, Trust in authority, privacy	Online, multiple choice questions, not representative of all countries
International Differences in Information Privacy Concerns: a Global Survey of Consumers	2003	Columbia Center for E-Business	Academic	1000 US, 1199 International	534 valid responses	Privacy concerns, international comparison	Online, multiple choice questions
Privacy 2.0: Personal and Consumer Protection in the New Media Reality	2009	Norwegian Consumer Council	Political	Norwegian internet users	1372	Consumer protection, consumer comprehension, data protection	Representative, online, multiple choice
Public Awareness Survey 2008	2008	Data Protection Commissioner of Ireland	Political	Irish public	1000	Public awareness and concern re: data protection and privacy	Representative, face to face, multiple choice
Pan-European Survey of Practices, Attitudes and Policy Preferences as Regards Personal Identity Data Management	2010	European Commission	Political	27 EU Member States	26,574	Attitues of personal data policies and management	Random sample, interviews, multiple choice questions
A Surveillance Society: Qualitative Research Report	2007	Information Commissioner 's Office, UK	Political	U.K.	72	Public conception of surveillance	12, 2 hour discussion groups; six respondents in each group (mix of men and women)
E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behaviour	2000	Humboldt University Berlin	Academic	N.A.	206 volunteers	Privacy attitudes and privacy behaviour online	Ethnograhic, participants observed in simulated online purchase
Flash Eurobarometer 225: Citizens' Perceptions of Data Protection	2008	European Commission	Political	27 EU Member States	27000	Broad consideration of public's feelings and concern re: data usage and data protection	Representative sample in each country, interviews by phone or face to face, multiple choice qsts

Title	*Year*	*Institution/ Author*	*Sector*	*Sample Universe*	*Sample size*	*Field(s)*	*Form of Survey*
Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union	2010	European Commission	Political	27 EU Member States	26,574	Broad consideration of public's feelings on electronic idenity, information society and data protection	Multi-stage, random sampling; inteviews conducted face to face at home; multiple choice questions.
Personal Data Project: An International Survey on Privacy and Surveillance	2008	Queens University Canada	Academic	Cross National	9606	Opinions on Surveillance and Privacy, Cross National Comparisons	Representative sample from each country, interviews, multiple choice questions

References

ACQUISTI, A. & GROSSKLAGS, J.:

- (2004): "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", In: CAMP, L. J. & LEWIS, S. (Eds); *The Economics of Information Security*, Dordrecht: Kluwer.

- (2005): "Privacy and rationality in individual decision making", *IEEE Security and Privacy*, 3, 26-33.

ALLWINGER, K. & SCHILLAB, J. M. A. (2008): Vertrauen der ÖsterreicherInnen in den Datenschutz, Baden, Austria, Oekonsult Communication & Consulting. http://www.oekonsult.eu/datensicherheit2008.pdf

BACKHOUSE, J. & HALPERIN, R. (2007): *A Survey on EU Citizen's Trust in ID Systems and Authorities*, FIDIS Deliverable 4.4, London, London School of Economics and Political Science.
http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf

BELLMAN, S., JOHNSON, E. J., KOBRIN, S. J. & LOHSE, G. L. (2004): "International Differences in Information Privacy Concerns: A Global Survey of Consumers", *The Information Society*, 20, 313–324.

BRANDTZAEG, P. B. & LÜDERS, M. (2009): *Privacy 2.0: personal and consumer protection in the new media reality*, Oslo, Norwegian Consumer Commission. http://forbrukerportalen.no/filearchive/report_privacy_social_media_1_.pdf

GELLERT, R. & GUTWIRTH, S. (2012): "Citizens' access to information. The data subject's rights of access and information: a data controllers' perspective", in: FRIEDEWALD, M. (Ed.), *Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data* (Deliverable 3). PRESCIENT Project.

GUTWIRTH, S., BELLANOVA, R., FRIEDEWALD, M., HALLINAN, D., WRIGHT, D., McCARTHY, P., JEANDESBOZ, J., MORDINI, E., VENIER, S., LANGHEINRICH, M. & COROAMA, V. (2012): *Smart Surveillance - State of the Art Report*, Deliverable 1, SAPIENT Project. http://www.sapient-project.eu

HALLINAN, D., FRIEDEWALD, M. & McCARTHY, P. (2012): "Citizens' Perceptions of Data Protection and Privacy", *Computer Law and Security Review*, 28, 263-272.

HARPER, J. & SINGLETON, S. M. (2001): "With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us". http://ssrn.com/abstract=299930

Landsdowne Market Research (2008): *Public Awareness Survey 2008*, Portarlington, Ireland, Data Protection Commissioner.
http://www.dataprotection.ie/documents/press/Survey08.pdf

MURPHY, O. (2007): *A Surveillance Society: Qualitative Research Report*, Report prepared for COI on behalf of ICO Wilmslow, Cheshire, UK.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf

SAMATAS, M. (2005): "Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture", *Surveillance & Society*, 3, 181-197.

SCHÜTZ, P. & FRIEDEWALD, M. (2011): "Cui bono from giving up or protecting privacy? A basic decision theoretic model", *Journal of Information Assurance and Security*, 6, 432–442.

SPIEKERMANN, S. & GROSSKLAGS, J. (2005): "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behaviour", *Communications of the ACM*, 48, 101-106.

STRICKLAND, L. S. & HUNT, L. E. (2005): "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions", *Journal of the American Society for Information Science and Technology*, 56, 221–234.

The Gallup Organization (2008): *Data Protection in the European Union: Citizens' perceptions*, Flash Eurobarometer 225, Brussels.
http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

TNS Opinion & Social (2011): *Attitudes on Data Protection and Electronic Identity in the European Union*, Special Eurobarometer 359, Brussels.
http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

ZUREIK, E., STALKER, L. H., SMITH, E., LYON, D. & CHAN, Y. E. (Eds.) (2010): *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, Montreal: McGill-Queen's University Press.