June, 2012

Citizens' Perceptions of Data Protection and Privacy in Europe

Dara Hallinan, *Fraunhofer Institute for Systems and Innovation Research*
Michael Friedewald, *Fraunhofer Institute for Systems and Innovation Research*
Paul McCarthy

Hallinan, Dara, Michael Friedewald, and Paul McCarthy, "Citizens' Perceptions of Data Protection and Privacy", *Computer Law and Security Review*, Vol. 28, No. 3, 2012, pp. 263-272.

CITIZENS' PERCEPTIONS OF DATA PROTECTION AND PRIVACY IN EUROPE

Dara Hallinan & Michael Friedewald[1]

Fraunhofer Institute for Systems and Innovation Research
Breslauer Straße 48, 76139 Karlsruhe, Germany
{firstname.lastname}@isi.fraunhofer.de
http://www.isi.fraunhofer .de

Paul McCarthy
Trilateral Research and Consulting LLP
22 Argyll Court, 82-84 Lexham Gardens, London W8 5JB, United Kingdom
paul.mccarthy@trilateralresearch.com
http://www.trilateralresearch.com

18 May 2012

Abstract:
Data protection and privacy gain social importance as technology and data flows play an ever greater role in shaping social structure. Despite this, understanding of public opinion on these issues is conspicuously lacking. This article is a meta-analysis of public opinion surveys on data protection and privacy focussed on EU citizens. The article firstly considers the understanding and awareness of the legal framework for protection as a solid manifestation of the complex concepts of data protection and privacy. This is followed by a consideration of perceptions of privacy and data protection in relation to other social goals, focussing on the most visible of these contexts - the debate surrounding privacy, data protection and security. The article then considers how citizens perceive the 'real world' environment in which data processing takes place, before finally considering the public's perception and evaluation of the operation of framework against environment.

[1] Corresponding author

Hallinan, Dara, Michael Friedewald, and Paul McCarthy, "Citizens' Perceptions of Data Protection and Privacy", *Computer Law and Security Review*, Vol. 28, No. 3, 2012, pp. 263-272.

CITIZENS' PERCEPTIONS OF DATA PROTECTION AND PRIVACY IN EUROPE

1. *Introduction*

This article is a meta-analysis of public opinion surveys on public understanding and knowledge of data protection and privacy in Europe. Considered against a background of technological progression and the increase of data flows, processing and importance, issues of data protection and privacy are increasingly significant at both the individual and societal levels. Despite this, and increased attention and efforts on the part of a variety of actors (often in the name of 'the public'), an understanding of how the public understand and approach these issues is conspicuously lacking and often appears replaced by superficial assumptions as to what 'the public' want or need.

The article firstly considers the understanding of the legal framework for protection and finding that whilst rights are well known, deeper knowledge of the framework and its function within a broader legal and social framework is relatively superficial. This leads to an undervaluation of privacy as a social value. Perceptions of privacy and data protection are then considered in light of security and surveillance, revealing a nuanced perception on the part of the citizenship and highlighting variation and features of trust and mistrust in authorities, a contextual approach to perception of surveillance measures and offering an elaboration of findings related to the unbalanced conception of privacy and data protection.

This is followed by a consideration of how citizens perceive the 'real world' environment in which data processing takes place. In terms of actors, the public generally show higher levels of trust in government than in the private sector. When considered in detail or with reference to aspects of surveillance, this trust is replaced by significant uncertainty and even mistrust. As opposed to the apparent familiarity with the actors involved in the data environment, an elaboration of the environment itself is not forthcoming. This is demonstrated for example, by the lack of clarity in public perception regarding responsibility allocation or issues of transborder data flows, revealing a superficial understanding of the environment and its logic after initial instances of collection. Consequently and perhaps due to the intangibility and invisibility of the environment, the public displays significant fear regarding data processing (and the development and significance of the data environment) and what this could mean for the individual and society. In terms of security and surveillance measures there is a similar feeling of uncertainty and fear regarding social impact, although as measures become more directed this fear appears to diminish. Despite this, the public seem to have resigned themselves to the increasing release of data as a necessity of life in the modern world. In terms of surveillance, surveys show general public opinion favouring more controls and more surveillance targetted at groups who already suffer from social and other forms of exclusion. There is thus a degree of cognitive dissonance, particularly considering the high abstract importance allocated to privacy. Considering limited information, bounded rationality and behavioural distortions present in a decision in a data environment, it appears that the public are being forced to act in an environment they have no template for approaching.

Finally, the public's perception of the operation of the framework against the environment is considered. The public feel they have lost control over their data and that there are enforcement and application problems. There is a desire for clarity, solidification and understanding of an environment perceived as complex and fluid.

1.1. A Note on Surveys

In general, public opinion surveys and their results are an imprecise tool in the creation of an image of a diverse public. They contain a series of potential flaws which can influence the reality and truth of eventual findings, including the presence of the motivation of key players in the survey process in the final findings and inherent flaws in survey methodology, such as bias created by flawed concept framing, question clarification and ordering, response rates and the legitimacy of the extrapolation of results from one group onto a wider population or vice versa. These methodological drawbacks can manifest significantly between surveys, particularly in the case of disputed issues (such as data protection and privacy), to the point of contradictory survey findings.

Whilst all the above issues are of relevance to the consideration of survey analysis in the context of this article, certain problems specific to the subject matter presented themselves as significant. Firstly, the surveys used in this article represent a variety of different approaches and scales and as such conclusions represent extrapolations from data which vary in compatibility. As the article 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 posed further issues in relation to the extrapolation of general conclusions from essentially local data.

Secondly, this piece seeks to identify main trends and create an understanding as to how the European public at large understand and view data protection and privacy issues. In this respect, 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 data protection and privacy 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 each factor may play a greater or lesser role in relation to each sub-issue.

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[2] for example, knowledge of the national Data Protection Authority varied from 51% in Hungary to just 16% in Spain. An expansion of this even reveals broader regional trends, for example a Scandinavian group perspective can be isolated. In the same

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

survey there is a separation made, 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.[3]

Even when a viewpoint appears to be identifiable, the complexity of the issues involved means this is never monolithic. Considering the fluidity of understanding in relation to the technical and social background, each view may be subject to qualification or change dependant on context of application or to circumstantial change.

2. *What Does the Public Know about Data Protection and Privacy?*

2.1. What Does the Public Know About the Current Protection Framework?

With overarching relevance, it is necessary to bear in mind that the philosophical and social justifications of the right to privacy (and data protection) are incredibly difficult to define and are constantly changing with the development of society and law. As Post declares, “privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all”.[4] Thus, even the use of legalislation as a certain manifestation is arguably in principle flawed. These ambiguities in understanding and definition at the most fundamental level influence the clarity of public perception. They are very likely reflected in uncertainty as to the relevance and operation of the framework generally, privacy’s relationship with a quickly developing background, the calculation of privacy’s relationship with other rights, with individual action and its relevance in light of other social goals.

From the survey results it is clear that 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. This trailed crime prevention by only 3%.[5]

It is immediately evident that there is confusion, or at least an apparent lack of distinction, between privacy and data protection, although this is not explicitly stated in any individual survey. Indeed many surveys appear to use the concepts interchangeably themselves. The privacy protection framework does not feature at all in respondents answers. Practically however, this can probably be explained. Firstly one can consider the subject matter of surveys considered and their bias toward issues of data processing. Secondly, in considering the symbiotic development and deeper justification for both rights there may be no need for the public to distinguish when considering broader

[3] For broad considerations of factors influencing privacy and data protection conceptions see Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers", *The Information Society*, Vol. 20, No. 5, 2004, pp. 313–324. Samatas, Minas, "Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 181-197. Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010.

[4] Post, Robert C., "Three Concepts of Privacy", *The Georgetown Law Journal*, Vol. 89, No. 2001, pp. 2087-2098.

[5] Landsdowne Market Research, "Public Awareness Survey 2008", Data Protection Commissioner, Portarlington, Ireland, 2008. http://www.dataprotection.ie/documents/press/Survey08.pdf.

issues. Finally, the data protection framework simply has a more tangible set of laws onto which to grasp and references as to its sphere of operation. It is unlikely, for example, that a respondent will be aware of ECtHR case law defining privacy's bounds.

Whilst there seems to be a considerable variation between European countries in relation to their knowledge of protection frameworks and the protections they offer, it is notable that the majority of Europeans appear familiar with the key rights the data protection framework offers. For example, although a citizen's right to access data held by others' was the least known amongst respondents, the EU awareness average still sat at 59%.[6] However, it must also be noted that knowledge levels dropped when respondents were questioned as to the more subtle, abstract or complicated aspects of protection, such as the status of sensitive data or the situation relating to cross-border data flows.

There is not the same level of awareness regarding National Data Protection Authorities (NDPAs). In the same Eurobarometer survey mentioned in the paragraph above[7], the EU average awareness of the existence of NDPAs sat at a low 28%. Amongst those aware of the existence of local NDPAs, there was still considerable uncertainty as to their remit and capability (whether or not they can impose sanctions for example). Although this may be partially explicable, assuming an individual who has not had cause to complain may not be expected to have found out about a national authority, these figures do not align with knowledge of aspects of protection. This suggests an imbalance in awareness between the letter of protection and its operation in fact. Taken in combination with a lack of awareness regarding certain of the more subtle aspects of protection and with points which will be made later regarding a lack of awareness of the social aspect of data protection, one could view the public's understanding as relatively superficial and limited to the letter of protection itself. It is thus no surprise that other more minor sectoral or supporting legislation made no appearance in any survey, nor were they brought up spontaneously by any lay respondent.

The status of data protection within the contexts of a wider legal order was rarely mentioned or apparently considered. On the one hand this may partially to be expected. Its elevation to the status of fundamental right has only been recent and through an instrument and means which may themselves not be so transparent or apparent to the individual citizen and the significance and consequences of this, both theoretically and practically are still uncertain. On the other hand, this is incongruent with an expected public awareness, understanding and familiarity with designated fundamental rights.

The above point brings into question how privacy and data protection within a wider system of law and society are understood and viewed. It is apparent that, although people are aware of the existence of rights they are not immediately aware of why they have manifested as they have, nor do they have appear to have given much thought to their social function. However when longer discussions ensued considering wider erosions of privacy and potential threats to individual data etc. participants began to voice fears based on the social dimensions of the rights, although they often found these difficult to elaborate and articulate. This perhaps demonstrates an imbalance in the public's concepts of privacy and data protection in relation to its dual individual and social function. This resonates with Solove's commentary, "Privacy is often cast as an

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

[7] Flash Eurobarometer 225, 2008 (fn 6).

individual right and balanced against the greater social good, which results in privacy being frequently undervalued".[8] There are factors which perhaps meditate toward making this so. Firstly, it is possibly not high on an individual's list of priorities to consider the social conception of any right, let alone rights as complicated and abstract as data protection and privacy. Secondly, the invisible and unknown environment in which data protection issues play out (this point will be returned to later) may make it difficult for the individual to conceive of social impacts, social importance or trace the consequences of aggregate action in a considered way. Finally, in considering the conception of the issue by the public, it is apparent that a number of reference points, for the conception of data protection (for example online shopping considered in "the Effect of Online Privacy Information on Purchasing Behavior")[9], come with a series of easily recognisable individual actions and trade offs, in which acts are seen in terms of isolated instances, as opposed to a reflection or involvement in issues which may have social significance.

2.2. Privacy, Data Protection and Security

The above analysis of an imbalanced conception is applicable to the evaluation of privacy and data protection in relation to other social goals. The most visible of these contexts is the debate surrounding privacy, data protection and security. Research in relation to these contexts has been extensive and reflective of vigorous academic and policy debates. As befits the relatively controversial nature of the research area, survey research and conclusions and the motivations to carry them out in the first place, at times diverge significantly. We present a synthesis of various surveys (and other pieces of empirical research) in the following paragraphs.

In '*A Surveillance Society: Qualitative Research Report*'[10], the author splits participant opinion into 3 attitudinal types, Acceptors, Authoritarians and Libertarians. The Libertarians, who formed the minority of the sample were those "who were more outward looking in their concerns, and more likely to think about society and their place in it". Unsurprisingly this group were significantly more concerned about a security privacy trade off and met the issue with a series of principle based democratic and social arguments. However, the other groups, whilst differing in approach, viewed privacy from a predominantly individual point of view, detached from its social significance.

Authoritarians approached privacy strongly as an individual right rather than as a social good. This led directly to a balancing action[11] in which other goals whose social 'importance' was more easily referable (or had at least been more continually referenced) were prioritized. This led to positions such as "national security ... and personal safety are of overriding importance: the common good is paramount", "the

[8] Solove, Daniel J., *Understanding privacy*, Harvard University Press, Cambridge, Mass., 2008a.

[9] Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research*, Vol. 2, No. 2, 2011, pp. 254-268.

[10] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

[11] 'Balancing' appears to be the predominant concept in many citizens' minds: If we want more security we have to give up privacy. Even if this is highly debated (or even rejected) in the academic community.

innocent will not be harmed or inconvenienced", "only the guilty are actively being watched, so I, as an innocent citizen, will not be 'picked out of the crowd' and if I am then I have nothing to hide".[12] In this set of arguments a broader set of consequences to privacy infringement is not present, in the blunt preference for security over privacy, many demonstrate a lop sided balancing process which fails to show a nuanced understanding of privacy's structural importance or the potential effects of increasing data flows and processing.

Finally, acceptors viewed the right to privacy from the narrow, individual perspective, without wider consideration as to its social significance, apparently out of practicality. The complexity of the environment in which the balance was being carried out and the necessity of involvement in day-to-day activities which carried risk, seemed to dull perception of social consequence. This led to positions such as "someone, somewhere, will be looking after our best interests", accordingly "there was an assumption that there 'must be' laws against extreme abuse of data, although respondents tended to be rather vague about who or what this might be", and "the state and security forces are not institutionally malign or corrupt in intent; indeed they are there to protect us, the innocent citizen"[13]. This reflects a certain concept of a paternalistic state, a concept often mirrored by broader trends in technology deployment. The claim is that development and deployment of technologies is done for the good of the citizen, who by nature of their uninformed status does not understand the nature of the issue or solution and therefore has a less valid concept of 'the correct path'. As a consequence their viewpoint and voice is systematically devalued or ignored in discourse.[14] Realistically, this approach may be expected from individuals who lead normal lives and may not have considered the issue or the relevant structures in great detail. Whilst these views undoubtedly also represent other issues such as the respondents trust for authority, this does not obscure the fact that data protection and privacy issues, particularly on a social level were simply a perception black spot. There is concern, but through lack of understanding of structure there is equally a powerlessness to react to it. There were thus necessary presumptions made about the nature of unclear structures that allowed practical functionality without structural clarity (this will be returned to later).

Other surveys exploring these themes give different perspectives. In terms of a comparative analysis, two Eurobarometer studies provide insight into pan-European concerns as well as the differences and commonalities in public attitudes towards these issues in Member States. We have already mentioned some of the findings of these studies. While data protection was the main focus of both studies, findings relevant to issues related to security can also be found in both reports, specifically in the sections exploring data protection in the context of international terrorism. An important point, noted in the executive summary of the Eurobarometer report on citizen's perceptions on data protection in the European Union, was that the public accepted that international terrorism would be one instance which would allow for the suspension or restriction of normal data protection rights. The figures reported here overall saw respondents agreeing that it should be possible to monitor passenger flight details (82%), telephone

[12] Murphy, Surveillance Society, 2007 (fn. 10).

[13] Murphy, Surveillance Society, 2007 (fn. 10).

[14] Spiekermann, Sarah, and Frank Pallas, "Technology paternalism – wider implications of ubiquitous computing", *Poiesis & Praxis*, Vol. 4, No. 1, 2006, pp. 6-18.

calls (72%) and Internet and credit card usage (75% and 69%, respectively) when this was for the purpose of fighting terrorism.[15]

However, the survey findings also suggested that citizens viewed government moves towards relaxing data protection provisions with distrust. The findings also reflected the comments made previously about the difference in perceptions when surveillance is seen as something to which ordinary citizens should be subjected. The survery found that around a third "stressed that only suspects should be monitored (27%-35%) and approximately one in five (14%-21%) wanted even stricter safeguards"[16]. Expanding on these averages, the survey reported differences between Member States. In response to the question as to whether people should be monitored when they fly in light of international terrorism, those supporting "unconditional monitoring of people's personal data" was highest in Hungary and the UK (53%). It was lowest in the Czech Republic (23%) and Finland (21%). In the Netherlands and Finland, 36% and 40% of respondents respectively stressed that only suspects should be targetted. In the UK and France, only 17% and 18% saw this as being necessary.[17]

Other surveys confirm that the public often sees surveillance positively when it seems targetted against threats. One interesting example are studies reporting on the views of the US public with regard to various surveillance and security measures. In the aftermath of 9/11, some surveys revealed high levels of support for surveillance measures and technologies but later surveys have revealed tensions between public attitudes and governmental surveillance practices. For example, a survey conducted by Harris International[18] in the aftermath of 9/11 found 90% of American citizens in favour of three or more new surveillance measures, such as the use of facial recognition and phone and Internet monitoring. Even highly intrusive measures such as cell phone call monitoring was supported by 54%. Compare these findings with a survey by Zogby International[19] which saw a decline to only 28% supporting routine call monitoring. This latter survey reported that only 38% of respondents believed that Americans had moved beyond a 9/11 mentality even though support for surveillance measures had declined. A reason for this could be decreasing levels of trust in the US government.

Trust in government and those controlling surveillance technologies and implementing surveillance practices is a critical feature of surveys. Generally, surveys report low levels of support in most countries. In relation to the US figures above, a recent survey by the Ponemon Institute[20] found that privacy trust in the US government declined from 52% in 2005 to 38% in 2010. In the UK, a 2010 study conducted on behalf of the Joseph Rowntree Foundation[21] found 65% worried about the UK government holding data on them, an increase from 53% in a 2006 study asking the same question. A study

[15] Flash Eurobarometer 225, 2008 (fn. 6).

[16] Flash Eurobarometer 225, 2008 (fn. 6).

[17] Flash Eurobarometer 225, 2008 (fn. 6).

[18] Harris Interactive, "Overwhelming Public Support for Increasing Surveillance Powers and, Despite Concerns about Potential Abuse, Confidence that the Powers Will be Used Properly", Press Release, 3 October 2001, Rochester NY, 2001. http://www.harrisinteractive.com/NEWS/allnewsbydate.asp?NewsID=370.

[19] Zogby International, "Voters Balance Privacy, Surveillance", Press Release, 6 February 2006, Utica, NY, 2006. http://www.zogby.com/news/2006/02/02/voters-balance-privacy-surveillance/.

[20] Ponemon Institute, "2010 Privacy Trust Study of the United States Government", Ponemon Institute, Traverse City, MI, 2010.

[21] ICM, "State of the Nation Survey 2010", Joseph Rowntree Foundation, York, 2010.

by the London School of Economics on national ID cards also found that trust was low for the suggestion that governments would protect and use data responsibly. Using a seven point scale, with 1 being strongly agree and 7 being strongly disagree, it found that the mean of responses was 5.9 for citizens trusting that governments would protect their data. Differences were also reported between European countries with the UK and Ireland being less trusting than respondents from central and eastern European countries.[22]

2.3. Public View of the Regulatory Environment

2.3.1. *Actors*

Surveys generally distinguished between state actors and private organisations. It is interesting to note that 'other individuals', whilst mentioned tangentially in relation to other questions such as those related to ID theft, were not seen as a body or entities worthy of specific consideration. This is particularly interesting considering the key role played by the individual in the online environment and the individual nature of many perceived threats. 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. For example, in 'Flash Eurobarometer 225'[23] medical services were highly trusted with an 82% positive trust rating, whereas local authorities scored a lower 67%. However, these numbers perhaps obscure a more nuanced understanding of the issue. 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 control and safeguard the data they have been given. This could be at least partly as a result of constant media coverage relating to authorities' leakage of personal data.[24]

Within the private sphere there is also considerable trust variation. In the same Eurobarometer survey, banks received a 66% trust rating (perhaps this would be different in 2011) whilst mail order companies received a trust rating of only 24 %.[25] However, despite these statistics, when deeper opinion was sought regarding commercial organisations handling of personal data, a distinct undercurrent of distrust emerged. Interestingly, whilst responses predominantly disapproved of sharing between government and private organisations there was little elaboration as to what the public believed was the model of interaction between organisations. There was equally little elaboration 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 superficial first instance of data collection.

2.3.2. *Responsibility Allocation*

[22] Backhouse, James, and Ruth Halperin, "A Survey on EU Citizen's Trust in ID Systems and Authorities", FIDIS Deliverable 4.4, London School of Economics and Political Science, London, 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf .

[23] Flash Eurobarometer 225, 2008 (fn. 6).

[24] Backhouse and Halperin, Survey, 2007 (fn. 22). This report considers trust in ID authorities' capability to handle data and further dissects citizen, authority trust relationships.

[25] Flash Eurobarometer 225, 2008 (fn. 6).

Following from this, the public does not seem certain which actors should be responsible for the safe handling of personal data and indeed opinion changes depending on the nature of entity 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. In relation to online shopping sites the percentages were 41% individual and 39% shopping site. 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 one 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). This allocation is, to some extent in contrast with the relatively harsh penalties the public seems to wish on organisations that breach standards. Considering the uncertainty as to who should hold responsibility it seems strange there should be preference for harsh regulation. 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 in the future.[26]

2.3.3. *Transborder Data Protection*

The public seemed equally uncertain as to how to approach the increasing globalisation of data flows. There was strong consensus that a harmonised set of data protection guidelines across the EU made sense and consequently that regulation at both national and EU levels was necessary. However, fewer people seemed aware of the issues arising from extra-territorial transfers or the risks this brought. In fact, even when data controllers were asked about their knowledge of the term 'standard contract clauses' 65% of respondents whose companies transferred data outside the EU were not aware of the term.[27]

2.3.4. *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.[28] This concern was relevant to both state and commercial organisations. It is curious however, that the number of people who reported actually falling victim to this is tiny in comparison to the apparent concern. 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 coverage the issue has been given in the media. Murphy points out that concern may be exacerbated by 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."[29] The public also demonstrated concern relating to the commercial collection and use of data. Unsurprisingly, the public approached the issue from an individual impact perspective and were concerned and annoyed by the perceived end results of data distribution,

[26] Special Eurobarometer 359, 2011 (fn. 2).
[27] Flash Eurobarometer 225, 2008 (fn. 6).
[28] Landsdowne, Public Awareness, 2008 (fn. 5).
[29] Murphy, Surveillance Society, 2007 (fn 10).

namely direct mail, spam, cold calling etc. Related to this, the public showed concern relating to certain data practices linked to this fear (but which also have wider significance), 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'.[30]

Although there were more abstract fears relating to the combination of data and/or databases, the development of a surveillance society and further issues related to assemblages of data etc., in terms of their social basis, 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".[31] 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'.[32]

2.3.5. *Justifications and Benefits*

Despite the above risk recognition and general uncertainty and the fact that 63% state that disclosing personal information is a big issue for them, individuals seem to accept the need to divulge increasing amounts of information.[33] The overarching reason for this acceptance is the rather deterministic viewpoint that it is 'simply part of modern life'. On the one hand, there is the perceived obligation to release more information, both 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 recognise 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).[34] When discussing rewards considering information imbalances and imperfections (see below) as well as behavioural aspects (preference for short term over long term considerations etc.) may be explanatory and significant.[35] The deterministic approach to obligatory information disclosure can arguably also be seen as a practical coping mechanism for significant power imbalances in the collection process. The processes are operating at a scale over which the individual feels very little control. Thus, formulating a position in response to increased collection may be difficult as goals and institutions may superficially remain the same, whilst the key mechanisms which drive the process are imperceptible. Trends and effects are detached in perception

[30] Special Eurobarometer 359, 2011 (fn. 2).
[31] Murphy, Surveillance Society, 2007 (fn 10).
[32] Special Eurobarometer 359, 2011 (fn. 2).
[33] Special Eurobarometer 359, 2011 (fn. 2).
[34] Brandtzaeg, Petter Bae, and Marika Lüders, "Privacy 2.0: personal and consumer protection in the new media reality", Norwegian Consumer Commission, Oslo, 2009. http://forbrukerportalen.no/filearchive/report_privacy_social_media_1_.pdf.
[35] Acquisti, Alessandro, and Jens Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in Camp, L. Jean, and Stephen Lewis (eds.), *The Economics of Information Security*, Kluwer, Dordrecht, 2004, pp. 165-178. Schütz, Philip, and Michael Friedewald, "Cui bono from giving up or protecting privacy? A basic decision theoretic model", *Journal of Information Assurance and Security*, Vol. 6, No. 5, 2011, pp. 432–442.

from the decisions and mechanisms driving them, creating the impression of inevitability.

2.3.6. *Privacy Protection*

It is remarkable that, considering the above, individuals do not use privacy enhancing technologies more. In Flash Eurobarometer 225, only 22% of respondents claimed to have used privacy enhancing tools, whilst 56% had never heard of the technology. Amongst the reasons cited were a lack of belief in their effectiveness or that respondents wouldn't know how to use or install them.[36] The European Commission noted this point in its communication on privacy enhancing technologies in terms of raising public awareness and increasing consumer use of these technologies.[37] It remains unclear however how far this objective has been achieved or what the impacts have been on rates of use and public knowledge.

However, individuals do claim to use a range of or other technology based techniques including altering browser or usage settings, deleting cookies or reading or ensuring privacy policies before trusting a website. In fact it was only 15% of Eurobarometer 359 respondents who claimed to do nothing to protect their online privacy. It is however, equally informative that when considering the specifics of these methods there was a significant knowledge gap between action, understanding and consequence. For example, when reading privacy statements there was a considerable lack of comprehension as to what they represented or what they meant when read in full (only a third claimed to understand them fully).[38]

Other strategies were also highlighted, including giving false information, refusing to give information and staying away from situations in which information may have to be given.[39]

2.3.7. *Uncertainty and Inconsistency*

Whilst figures can be put on certain aspects of opinion in individual surveys, there is considerable difference between actual behaviour and opinion. For example, this has been shown to be the case with respect to the stated importance of privacy in online environments and behaviour in relation to privacy protection (reading privacy statements for example).

It seems from the above answers that, when considering structural or more abstract issues (transborder data flows for example), the public displays a greater uncertainty than when considering issues with direct individual relevance (spam etc.). This suggests that the model for understanding what happens with data once it is released by the individual, or what this means on an aggregate scale, is rather fluid and uncertain.

[36] Flash Eurobarometer 225, 2011 (fn. 2). London Economics, "Study on the economic benefits of privacy−enhancing technologies (PETs)", Final Report to the European Commission DG Justice, Freedom and Security, London, 2010. http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

[37] European Commission, "Promoting Data Protection by Privacy Enhancing Technologies (PETs)", COM(2007) 228 final, Brussels, 2007.

[38] Special Eurobarometer 359, 2008 (fn 2).

[39] There have been privacy studies which suggest that the responses stating they protect privacy are significant overrepresentations, the above figures may thus be more indicative of what people believe they ought to do rather than what they in fact do

The data environment can be perceived as consisting of two parts; supporting technological infrastructure (and its innate capabilities) and the operation of the network of data connections and flows that constitute its lifeblood. In each consideration of technology, the public showed a significant lack of awareness as to the capabilities, uses and key privacy impacting features present. This is demonstrated well in the U.S. survey, 'Technology, Security and Individual Privacy: New Tools, Threats and New Public Perceptions'.[40] A lack of understanding as to the shape and operation of the data flows themselves is demonstrated in 'Privacy 2.0: Personal and Consumer Protection in the New Media Reality'.[41] Here it is pointed 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 questions of relevance which are unclear. 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.[42] Although they are aware of their significance, the public may not yet have the reference points to answer these questions solidly.

Acquisti and Grossklags consider the possibility that "Privacy in theory may mean many different things in practice" and consequently that "the parameters affecting the decision making process of the individual are perceived differently at the forecasting (survey) and operative (behavior) phases". They isolate a series of potential limiting factors to the individual decision to balance a transaction with a potential information security impact. The decision making model may be unbalanced by limited information, bounded rationality issues, self-control problems and other behavioural distortions. The lack of understanding of the data environment mentioned above would certainly account for impacts on each of these factors and thus significantly reduces the ability for the individual to 'rationally' balance each action.[43] Consequently, awareness of issues, such as the importance of privacy and data protection, and what can be done etc., on an abstract scale may not translate to the apparently corresponding action in concrete situations.

Thus, whilst not unaware of dangers and the existence of structures through which data processing and protection operate, there is a lack of understanding as to how and why they operate. This provides little basis for practical decision making in an environment in which increasing data collection and dissemination is perceived as a necessity for participation in everyday acts as well as society in general.

The broader consequences of this are, firstly, that citizens are unable to formulate considered responses, even to identified issues, as they only have half of the relevant foundations through which to do this. Secondly, the public may be vaguely aware of, but largely unable to consider responses to a series of other threats. Firstly, the tangible impacts which are not obviously related to original data collection are ignored.

[40] Strickland, Lee S., and Laura E. Hunt, "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions", *Journal of the American Society for Information Science and Technology*, Vol. 56, No. 3, 2005, pp. 221–234.

[41] Brandtzaeg et al, Privacy 2.0, 2009 (fn 35).

[42] Allwinger, Kristin, and Joschi M. A. Schillab, "Vertrauen der ÖsterreicherInnen in den Datenschutz", Oekonsult Communication & Consulting, Baden, Austria, 2008. http://www.oekonsult.eu/datensicherheit2008.pdf.

[43] Acquisti and Grossklags, Privacy Attitudes, 2004 (fn, 36).

Secondly, as the data processing itself is invisible and the processes largely not understood, the increasingly broad impact data processing has on other systems (social, economic etc.) is correspondingly invisible. Finally, a lack of understanding of the processes means the processes themselves develop without a public presence to consider and monitor their potential and direction. The split between the necessity to operate within but the lack of understanding of, the structures of the information society is increasingly making the public feel powerless and confused. This brings to mind Solove's applied reading of Kafka, "In *The Trial*, the problem is not inhibited behavior, but rather a suffocating powerlessness and vulnerability created by the court system's use of personal data and its exclusion of the protagonist from having any knowledge or participation in the process. The harms consist of those created by bureaucracies—indifference, errors, abuses, frustration, and lack of transparency and accountability".[44] The bureaucracy here works as a metaphor for the broader data environment with its own systems and order. Although the dystopic image is certainly diluted by the plurality of actors and their lack of coordination, from an individual perspective the effect retains some similarity.

2.4. Effectiveness of Regulation in Light of Environment

From the above it is clear that there is a certain knowledge shortfall in understanding of the framework and the environment it is designed to regulate. The aggregated uncertainty this creates can make it difficult to isolate specific expectations as to how and to what extent protection is expected. As a consequence there is very little survey information on what or how the public feel is wrong with the framework or how it could be improved. This may, in itself, be indicative of a greater issue, as the public should be better able to comprehend their legal protection.

Within this uncertainty however, the elements of protection offered are well known and the relevance of each aspect is understood and generally agreed to be important. Considering these aspects to reflect deeper principles, it is possible to suggest that the public (whilst perhaps not having specifically considered it) do generally support the framework and its principles. A reflection of this is shown in organisations' perceptions of the effect of the DPA on consumer trust, 85% believing it had a positive effect.[45]

Yet, from the available data there is a general feeling that personal data does not receive the protection it should. Demonstrated most obviously by the fact that a large majority feel they have lost control over their data as well as other opinions on protection. For example, in Flash Eurobarometer 225 a majority of respondents believed that national legislation could not cope with the demands currently placed on it.[46] Whilst principles seem not to be disapproved of, protection in reality is not perceived to be of the same quality.

It would therefore be logical to suggest that it is in the enforcement and application to the data environment, and by extension the change and fluidity of this environment, in which problems are perceived to lie. That the public see a problem in enforcement is

[44] Solove, Daniel J., ""I've got nothing to hide" and Other Misunderstandings of Privacy", *St. Diego Law Review*, Vol. 44, No. 2008b, pp. 745-772.

[45] Social and Market Strategic Research, "Report on the Findings of the Information Commissioner's Office Annual Track 2010: Organisations", ICO, London, 2010. http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_organisations.ashx.

[46] Flash Eurobarometer 225, 2008 (fn. 6).

demonstrated by the desire for relatively harsh measures for organisations which breach norms, whilst the uncertainty of application against the complicated current environment is demonstrated in the discrepancy and uncertainty in defining terms for even relatively basic concepts such as responsibility allocation.

Whilst (possibly due to the complexity of the environment making an appreciation of how the framework should apply very difficult) the question as to how to remedy the situation has been only briefly considered in surveys. However, there are certain instructive opinion trends which unsurprisingly all move toward clarification of the environment and the operation of the framework in relation to it. Firstly, there is a desire for greater education about the principles and processes of the framework and environment. Secondly, there is a desire to solidify the fluidity of the environment (or at least elements of it), for example, 64% of Europeans believe data would be better protected by organisations if they were obliged to have a specific contact person responsible for the correct handling of data, whilst Austrians often spontaneously and outside the survey questions suggested the need for a 'one stop national authority' to be set up, which could, when asked, research and provide information about the dispersion of citizen information.[47]

When measures were put in more solid terms to Data Controllers, the same concerns were applicable and high proportions promoted more specific measures aimed at removing uncertainty such as 'more harmonized rules on security measures', 'further clarification on the practical application of some of the key definitions and concepts of the European Directive and national data protection laws'.

3. Conclusion

As technology and data processing play a greater role in the life of the individual and society, they gain increasing significance in the shaping of the social environment. This potential makes them an inevitable policy battleground. Accordingly, in a democratic society, participation should play a role in each policy approach, initiative or decision. However, whilst 'public opinion' is often cited as legitimation for measures and discourses aiming in myriad directions, an understanding of how the public understand and approach these issues, that is to say an understanding of what this 'public opinion' actually is, is conspicuously lacking.

Public understanding of the legal framework was taken as a solid starting point for consideration of the complex and fluid issues of data protection and privacy. It was immediately apparent that the public still place a high value on the idea of privacy and data protection. In line with this, awareness of the main tenets of the protection regime was high. However, it was also apparent that an understanding of the regime did not stretch far beyond this, as knowledge of deeper aspects of protection was rarely forthcoming. There was equally a disconnection between the abstract perception of importance and how, and to what end, the data protection frameworks fit into a broader system of law and society. This was perhaps best exemplified by the lack of awareness of data protection as a fundamental right. Accordingly there was an undervaluation of privacy as a right with social value in comparison to its perception as an individual right.

[47] Allwinger and Schillab, Vertrauen, 2008 (fn. 43).

Following this, perceptions of privacy and data protection were considered in light of their relation to other social goals. The most visible of these contexts is the debate surrounding privacy, data protection and security. Whilst survey results differed significantly, they generally presented a nuanced perception on the part of the citizenship, highlighting variation and features of trust and mistrust in authorities and a contextual approach to the perception of security measures. In this respect, 'the public' may have a considerably more nuanced approach than many policy makers may think. However, once again, whilst privacy and data protection were seen as important, the disconnection between abstract importance and how, and what, this should mean in reality was apparent. Thus, the above analysis of an undervaluation of privacy as a social value was also found applicable in the evaluation of privacy and data protection as they relate to security. The public appeared to have difficulty in concretising abstract concepts of privacy and data protection and their social value against the apparently more concerte social goals of security.

Perception of the reality of the environment in which data protection finds expression as a right was then considered. In terms of the composition and nature of actors involved in the environment, higher trust was shown in government than in private sector actors, although, when considered in more depth there appeared to be an undercurrent of distrust related to both sectors. Whilst the public disapproved of the idea of data sharing between private and public sectors, there was little sense of being able to elaborate an actual model of data flows, either between sectors, or in fact at all. In essence, there was little elaboration of a model beyond the superficial first instance of data collection. Consequently, when considering more abstract issues related to the operation and consequences of data flows, such as responsibility allocation or issues related to transborder data flows (issues which are currently major challenges and will remain so in the future), responses became less certain and even contradictory. This reveals a superficial understanding of the environment and its logic after initial instances of collection. This lack of clarity feeds uncertainty, and the public thus displays significant fear regarding data processing and the potential consequences for the individual and society. In terms of security measures a similar uncertainty and fear regarding social consequences manifests. Despite this, the public deterministically accept an increase in the release of data, simply as a necessity and consequence of life in the modern world.

The model for understanding what happens with data once it is released by the individual, or what this means on an aggregate scale, is thus fluid and uncertain. In this respect, the inability of the public to concieve of the operation of either the technology and software forming the infrastructure, or what the shape, quanitity or consequences of data flows and processing might look like in reality, was conspicuous. This sheds light on the imbalance in conception of data protection as an individual right as opposed to a right which also has social value. Whilst data protection and privacy are found abstractly important, the mechanics by which impact manifests, either at individual or social level, are poorly understood and largely invisible. Thus whilst each individual's action is clear, the consequences and systems which transform action into consequence are not. Thus the public has a poor basis from which to form a picture of data relationships, consequences, issues and how they manifest, or to build a concept of the importance of these data flows in relation to other social structures or issues. There is thus a degree of cognitive dissonance, particularly considering the high abstract importance allocated to privacy. Considering limited information, bounded rationality and behavioural distortions present in a decision in a data environment, it appears that the public are being forced to act in an environment they have little template for approaching.

Finally, the public's perception of the operation of the framework against the environment is considered. The public feel they have lost control over their data and that there are enforcement and application problems. There is a desire for clarity, solidification and understanding of an environment perceived as complex, fluid and lacking in transparency.

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.