Watching me, watching you: Privacy attitudes and reactions to identity card implementation scenarios in the United Kingdom

JIS Accepted for Publication
Released: *2nd December 2005*
Accepted for publication in the Journal of Information Science: http://jis.sagepub.co.uk

Adam N. Joinson; Carina Paine

Institute of Educational Technology, The Open University, UK

Tom Buchanan

Department of Psychology, University of Westminster, UK

Ulf-Dietrich Reips

Department of Psychology, University of Zurich, Switzerland

Correspondence to: Adam Joinson, Institute of Educational Technology, The Open University, Walton Hall Campus, Milton Keynes, MK7 6AA . E-mail: a.n.joinson@open.ac.uk

Abstract

In the United Kingdom, government proposals for the introduction of an identity (ID) card have raised considerable privacy concerns. In the present research, opinions and attitudes about different ways of implementing ID cards are examined using an experimental methodology. Specifically, the level and type of compulsion and application process, and the use of a centralised database or trusted third party to hold personal information, are compared for attitudes towards ID cards. Moreover, the impact of implementation scenarios on people with different privacy concern profiles is examined. The results show that an implementation that combines high compulsion with a centralised database (the approach currently favoured by the UK Government) lead to the greatest negative shift in attitudes towards ID cards. Implementations proposed by others (e.g. the London School of Economics) show significantly less negative shift in attitudes. People's pre-existing privacy concerns also influence their evaluation of the different implementation scenarios.

Keywords: Privacy; Identity Cards

JIS Editorial Process
Received: 3rd November 2005
Revised: 1st December 2005
JIS-0276 Version 3.0

1. Introduction

The collection of personal information through highly portable means is becoming increasingly popular throughout numerous governments and businesses [1]. For example, through the use of smart cards, radio frequency identification (RFID) tags and ID cards. However, there are many fears concerning these information collecting technologies, in particular related to privacy.

In May 2005, the United Kingdom (UK) Government introduced its Identity Card Bill. This proposed legislation has raised concerns amongst civil liberty, privacy and data-protection groups (see [2]) – in part due to the likely high cost of the card, but particularly because of the development of a centralised 'National Identity Register'. The creation of a national identity register is unprecedented in the Western world, and there are concerns that its use would violate privacy [3]. This database will contain up to 51 pieces of information about an individual, including current and past addresses. Research into ID cards has also highlighted the need for a detailed consideration of data protection concerns in order for privacy to be supported [4]. For instance, each time the proposed National Identity Register database is queried, a footprint is left on the system, posing a possible privacy threat [5]. Moreover, the use of a centralised database to manage the National Identity Register has led to a number of security-based concerns (e.g. [6]), including the possibility that it would be a 'honeypot' for hackers and those engaged in identity theft. Despite these concerns, the UK Government claims 75% support for its proposed ID Card legislation [7], although this figure is disputed [2].

People's acceptance (or otherwise) of the collection of personal data is not simply decided by the type of information collected, and how it is stored and queried. Researchers have identified issues of trust [8,9], privacy concern [10], potential benefits [11, 12] past experiences [8], cultural attitudes [13] and government initiated consultation [13] as important in deciding whether or not a person is comfortable with disclosing personal information.

A further critical issue with regards to ID Cards may be that of control – not only over whether or not one would wish to divulge information or not, but also knowledge of what information about oneself is stored and by whom. Culnan and Armstrong [14] describe two types of privacy-related control: *environmental control* - an individual's privacy may be compromised if unauthorized access is gained to personal information as a result of a security breach or an absence of appropriate internal controls; and *control over secondary use of information* - computerized information may be readily duplicated and shared, and there is the risk of secondary use, that is information provided for one purpose may be used for unrelated purposes without the individual's knowledge or consent. Secondary use includes sharing personal information with others who were not a party to the original disclosure.

A second issue related to people's acceptance of a National Identity Card and Register may be their pre-existing privacy attitudes. There is a large body of research from the e-commerce field to suggest that people's privacy concerns limit their use of the Internet for shopping [15] and that privacy concerns in general are increasing.

Research has also shown that attitudes towards privacy are an important factor when considering the acceptance of smart cards [13].

As might be expected, privacy attitudes are subjective measures - varying from person to person based on individual perceptions and values. One scheme for categorising the different levels of privacy concerns is the Westin privacy segmentation [16]. The Harris Poll is a privacy survey conducted by telephone across the United States among approximately 1,000 people. This survey has been conducted regularly since 1995 and divides respondents into one of three categories depending on their answers to three statements. The three categories of respondents are:

The Privacy Fundamentalists,

Privacy fundamentalists view privacy as an especially high value which they feel very strongly about and they usually have high levels of distrust. They tend to feel that they have lost a lot of their privacy and are strongly resistant to any further erosion of it. Currently about a quarter (35%) of all adults are privacy fundamentalists [17].

The Privacy Pragmatists

Privacy pragmatists also have strong feelings about privacy and tend to have medium to high levels of distrust. They are very concerned to protect themselves from the misuse of their personal information by other people and organisations. They weigh the value to them and society of providing personal information and they are often willing to allow people to have access to, and to use, their personal information - where they understand the reasons for its use, can see the benefits for so doing and when they believe care is taken to prevent the misuse of this information. Currently around approximately 55% of all adults are privacy pragmatists [17].

The Privacy Unconcerned

The privacy unconcerned have no real concerns about privacy or about how other people and organisations are using information about them. They usually have low to no levels of distrust. Approximately 10% of all adults are privacy unconcerned [17].

In the present research, we consider people's privacy concerns in light of possible ways in which ID Cards could be implemented in the UK.

1.1 ID Cards: Possible implementations

Although the UK Government proposes a non-compulsory card, the proposed legislation allows the cards to become compulsory after a trial period, and few expect them to remain voluntary. At the time of the research, the main issue raised in public discussions of ID cards was the likely cost – the government estimate of £93 per card

has been challenged by a report by 14 academics at the London School of Economics (LSE), who propose a likely cost of between £170 and £300 [18].

The LSE has developed an alternative blueprint for the implementation of national ID cards that, amongst other aspects is, a) not as 'compulsory' as the government approach as outlined in the proposed legislation, and b) does not require a centralised database. In the LSE proposal [19], information is kept on the card itself (and backed up on a computer held by a trusted third party such as a bank, police station or solicitors). Unlike the government proposal, which would use processing centres to collect biometric data, the LSE proposal envisages the use of kiosks which individuals use at a time of their own choosing.

In its response to the LSE blueprint, the UK Government [20] argues that, 'The LSE scheme would not gain public trust' (p. 1), and that the use of kiosks, 'would be less private and secure … would not inspire public trust' (p. 9). The UK Government also conducted a conjoint analysis that found circa 70% support for its view of how ID cards should be implemented (p. 11). This study, conducted on behalf of the UK Home Office, however, only presented differing options regarding cost [21], while maintaining other factors stable, and did not mention the National Identity Register (i.e. the centralised database). As stated above, trust is a critical issue in the disclosure of personal information [8,9]. Research has shown that a lack of transparency and accountability of the collection and use of personal information may create high levels of distrust. This lack of trust can, in turn, affect the adoption and use of information collecting technologies, such as smart cards [13]. Interestingly, research into the government and privacy in the UK [22] has shown that this struggle to balance data sharing and the right to privacy is ongoing.

The aim of the present research is to consider ways in which the Home Office and LSE proposals differ – specifically, the ways in which an ID card application is made, and the location of the personal information. Although the proposals differ in many different ways, these can be seen as critical because a) the National Identity Register or centralised database is seen by many privacy campaigners as the weak link in the government scheme, while the UK Government proposes that the LSE model is inherently less secure than their proposal because of the use of trusted third parties, and b) the way in which an ID card is applied for (e.g. at a kiosk versus processing centre) is symptomatic of the differences between the two approaches, in particular the issues of control over the type of biometric identifier chosen and the location and timing of application.

Moreover, we know little about the links between people's attitudes towards privacy in general, and their attitudes towards ID cards. As well as comparing different implementations of ID cards, the present research also seeks to examine the impact of alternative implementations on people holding differing attitudes towards personal privacy.

2. Participants and Methodology

Participants were 1143 members of a research panel of Open University (OU) students called 'PRESTO' (the OU is an adult distance learning institution with nearly all students studying part time from home or work). In total 1935 members of the research panel were invited by e-mail to complete the web-based survey (response rate: 59%).The PRESTO panel demographic is slightly older than the average OU student, and slightly more females joined the panel than would be expected based on the gender balance in the target population. Panel members study a range of subjects at the OU. The study was conducted during the first reading in the UK Parliament of the proposed Identity Card legislation, and was closed at 1pm on the day the legislation was passed.

Data were cleaned by the removal of responses with more than half the data missing (n=17), or where the participant identifier carried via an encrypted URL (n=6) did not transfer successfully. This led to a final number of responses of 1122. Of these, 40% (442) were male, 60% (672) were female (demographic data unavailable for 8 participants). The mean age of the sample was 42.3 years, (range: 17 – 84 years, SD = 11.1).

2.1. Westin Privacy Segmentation

Participants responded to three questions used to identify their general privacy attitudes and to enable segmentation of the sample (see Table 1, below for the questions and scale). This methodology has been used extensively by the Harris Polling organisation [23], and was developed by privacy expert Alan Westin [24].

In line with the terminology and method used by Westin-Harris, participants giving privacy-oriented responses to all three questions were categorized as 'Privacy Fundamentalists'. Participants giving privacy-oriented responses to some, but not all, of the questions were categorized as 'Privacy Pragmatists', and participants giving non-privacy oriented responses to all the questions, were categorized as 'Privacy Unconcerned'.

Any participants (n = 9) who did not answer all three Westin segmentation questions were excluded from the segmentation process. The percentage of participants responding to each question is shown in Table 1.

Table 1. Responses to the Westin questions

	Strongly agree	**Somewhat agree**	**Somewhat disagree**	**Strongly disagree**
Consumers have lost all control over how personal information is collected and used by companies	12.1%	39.9%	44.6%	2.4%
Most businesses handle the personal information they collect about consumers in a proper and confidential way	5.1%	54.8%	32.6%	7.0%
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today	2.4%	44.6%	39.9%	12.1%

Using the segmentation process outlined above, Table 2 shows the percentage of participants categorized within each privacy category.

Table 2. Westin privacy segmentation

Westin Privacy Category	% participants
Privacy Unconcerned	11.6%
Privacy Pragmatist	55.9%
Privacy Fundamentalists	32.5%

The figures in Table 2 differ somewhat from recent Harris polls [25] – the respective percentages from the US in the 2003 poll are 10% 'Unconcerned', 64% 'Pragmatist' and 26% 'Fundamentalist'. However, Westin [23] has produced figures comparable to our UK sample: 37% classified as 'Fundamentalist', 52% 'Pragmatist' and 11% 'Unconcerned' (although it is unclear what survey data these figures are based on).

Treated as a scale, the three Westin segmentation items did not exhibit high internal consistency (alpha = 69.9), although it can be viewed as acceptable.

2.2. ID Cards in the UK

Participants were asked to respond to the question, 'The United Kingdom Government is planning to introduce Identity Cards and a National Identity Register. What is your attitude to this proposal?' using a 7-point scale anchored at 'Strongly against ID cards' and 'Strongly in favour of ID cards'. They were also asked 'How certain are you about your attitude towards ID cards in the UK?' as a measure of attitude strength (7-point scale, anchored at 'Very certain' and 'Very uncertain'). Participants who were not UK citizens, or who did not live in the UK, were excluded from any analyses of ID card attitudes (n = 91, 8.1% of the sample).

2.3. Implementation of ID Cards

The aim of the present study was to examine various systems for implementing ID Cards. Participants were told:

There are various ways in which an identification card system can be operationalized. Please read the outline below carefully, and imagine what your attitude towards a UK-wide identity card would be if the system were like this. Please assume that Identity cards would be compulsory, not voluntary.

This was then followed by an implementation scenario. The scenario proposed varied across two dimensions, based on differing options proposed by the UK Government and the LSE [19]. Each scenario was tested for ease of understanding, and matched for word-count. The component parts of the scenarios were:

High compulsion: A government agency would tell you to report with existing documents (e.g. birth certificate, passport, national insurance number) to a named processing centre at a specified time. You would need to allow yourself to be fingerprinted, have your iris scanned and your photograph taken. If you did not attend, or if you did not allow your biometric data to be recorded, you would be fined up to £2500.

Low compulsion: To get an identity card, you would visit a post office and enter a kiosk at the time of your choosing. You would choose the biometric identifier you wished to use (e.g. fingerprint, digital photograph or iris scan). The kiosk would automatically generate a form, which you would get validated by two people in a position of trust. You then send this form to receive your card.

Centralised database: The biometric identification, along with information like your name, date and place of birth, current and all previous addresses and driving licence number and expiry date (along with other relevant information) would be stored in a centralised government database. This database would be held securely by the government, and could be queried by all other government departments, the police, public service providers (e.g. NHS) and approved private sector organisations (e.g. banks, employers).

No centralised database: The biometric identification, along with information like your name, date and place of birth, current and all previous addresses and driving licence number and expiry date (along with other relevant information) would be held on your card and backed up locally in a secure database maintained by a trusted third party (e.g. a bank, police stations or solicitors). A centralised government database would hold only your name and an identifier.

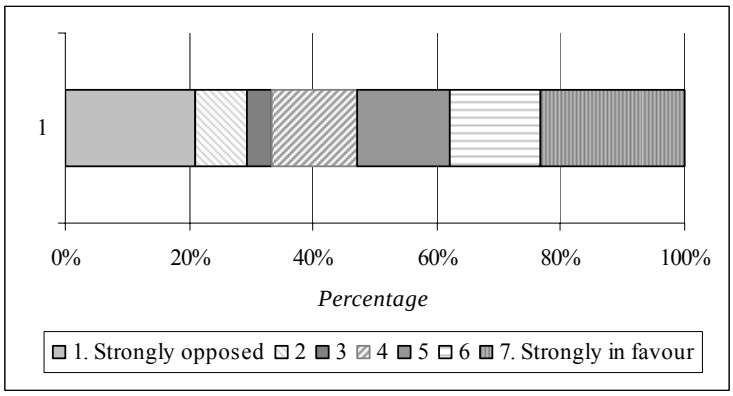
The scenarios were combined, such that all possible combinations of level of compulsion and type of database were presented. The order of the scenarios was also counter-balanced, so that in half of the scenarios the compulsion information was presented first, then the database, and in half the pattern was reversed. This led to eight possible combinations of compulsion type, database and order (2x2x2). The panel was randomly divided into eight sub-groups, and each group directed to a different scenario. Thus, each participant only responded to a single scenario. Following the scenario, participants were asked 'If this were the way in which ID cards were to be introduced, what would your attitude towards identity cards in the UK be?' and 'How certain are you about your attitude towards ID cards if this scenario were the one introduced?' using the same scales for the pre-scenario measures. A measure of attitude shift was calculated by subtracting the scenario attitude score from the pre-scenario attitude, such that a negative score meant a shift against ID cards, and a positive score, a shift in favour of ID cards.

Participants were also asked to respond to questions about their Internet use and any Internet-related privacy concerns and privacy behaviour. This data is not described in the present paper.

3. Results

The mean score on the 7-point attitude scale was 4.30 (SD = 2.24), indicating that participants were inclined to be in favour of ID cards. These attitudes were also held with a degree of certainty (Mean = 5.58, *SD* = 1.67). The distribution of attitudes was unusual – participants tended to score across the range of pro-ID card responses, but were clustered on 'strongly against' if anti-ID cards (see Figure 1).

Fig.1. ID card attitudes: Distribution



So, 63% of those opposed to ID Cards scored in the 'Strongly opposed' category, while only 44% of those in favour of ID cards scored in the 'Strongly in favour' category. The level of certainty with which pro- and anti-ID card attitudes were held was effectively the same (Mean = 5.85, *SD* = 1.77 for pro-ID and Mean = 5.88, *SD* = 1.30 for anti-ID) with only people responding in the centre of the scale exhibiting any uncertainty (Mean = 3.82, *SD* = 1.57).

Within the category of 'Privacy Fundamentalist', there was a fairly even split between those in favour and against ID Cards (see Table 3), with a slight majority in favour of ID cards. Amongst the 'Privacy Unconcerned' and 'Privacy Pragmatists', the majority were in favour of ID cards in the UK.

Table 3. Westin segmentation and ID cards

	Attitude to ID Cards in the UK: % and (N)		
Westin Categorization	**Anti-ID cards**	**Undecided**	**Pro-ID cards**
Privacy Unconcerned	32.5% *(37)*	9.6% *(11)*	57.9% *(66)*
Privacy Pragmatists	30.8% *(173)*	13.2% *(74)*	56.0% *(315)*
Privacy Fundamentalists	38.5% *(125)*	16.6% *(54)*	44.9% *(146)*
Means (N)	*33.5% (335)*	*13.9% (139)*	*52.6% (527)*

A chi-square test of association confirmed the uneven distribution of attitudes towards ID cards and Westin categorization ($X^2 = 12.61$, df = 4, $p<0.01$). A one-way analysis of variance (ANOVA) was calculated to examine scores on original attitudes towards ID cards by level of privacy concern. This analysis confirmed ($F_{(2, 997)} = 4.21$, $p<0.05$, $\eta^2 = 0.08$) that attitudes were statistically significantly more negative for those classified as 'Privacy Fundamentalists' (Mean = 4.00, *SD* = 2.32) than for the 'Privacy Unconcerned' (Mean = 4.49, *SD* = 2.22) and 'Privacy Pragmatists' (Mean = 4.43, *SD* = 2.17).

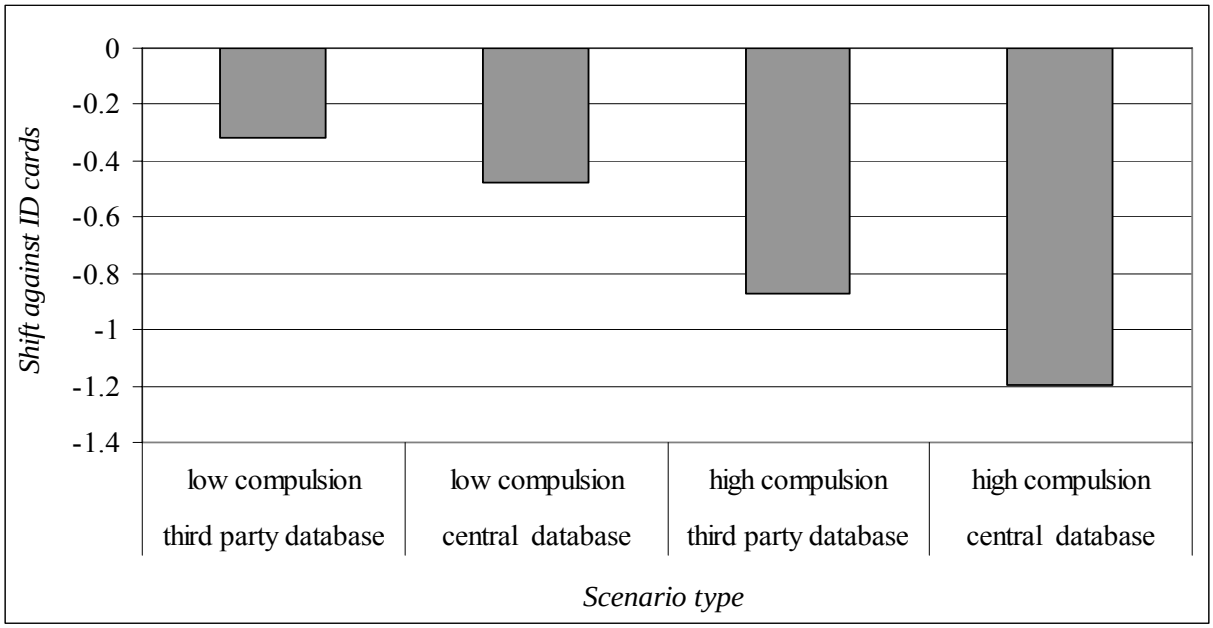
3.1. Attitude change and implementation scenarios

Regardless of the type of implementation scenario, attitudes towards ID cards moved towards the 'against' end of the scale following the scenarios. This is perhaps unsurprising since none of the proposed benefits of ID cards were presented in the scenarios.

The largest shift against ID cards was when the level of compulsion was high (e.g. no choice when to go for the biometric scanning, possible fines) combined with a centralised government database. This scenario approximates the current UK government view of how ID cards should be implemented. The average move against ID cards in this scenario was 1.2 points on the 7-point scale (see Figure 2).

The smallest shift in attitudes against ID cards was when the level of compulsion was low (e.g. going into a booth in a post office, sending the form yourself), combined with no centralised database. This scenario approximates an alternative view of how ID cards could be implemented as proposed by the LSE. The average move against ID cards in this scenario was 0.35 points on the scale (see Figure 2).

Fig.2. Attitude shift following scenarios



3.2. Privacy and Reaction to different scenarios

Of particular interest was whether or not the impact of the different scenarios differed according to people's general privacy attitudes. A linear regression was conducted to predict post-scenario attitudes to ID cards based on the type of scenario, pre-scenario attitudes (direction and strength) and Westin Privacy score (scale rather than segment). This regression confirmed that all five variables (although the Westin score was only marginally so) exerted a significant effect on post-scenario ID card attitudes (see Table 4, $R^2 = 0.69$), and that the impact of the scenario was independent of people's pre-existing privacy concerns or pre-scenario attitudes.

Table 4. Regression results (outcome variable: post-scenario attitude)

Variable	Beta	p	
Pre-scenario attitude	0.808	p<0.001	Positive pre-scenario attitude leads to more (relatively) positive post-scenario attitude
Compulsion	-0.122	p<0.001	High compulsion leads to more negative attitudes
Database	-0.055	p<0.01	Centralised database leads to more negative attitudes
Westin score	-0.034	p=0.055	Higher score leads to more negative attitudes
Certainty (pre-scenario attitude)	0.107	p<0.001	Higher certainty leads to more positive attitudes

More detailed analysis using a three-way ANOVA (compulsion X database type X Westin segmentation, n = 1001) showed statistically significant main effects of database type ($F_{(1, 988)} = 6.04$, $p<0.05$, $\eta^2 = 0.06$, centralised database led to more negative attitudes) and privacy attitudes ($F_{(2, 998)} = 3.81$, $p<0.05$, $\eta^2 = 0.08$, 'Privacy Fundamentalist' more opposed than other groups) on post-scenario attitudes. The main effect of level of compulsion approached significance ($F_{(1, 988)} = 3.43$, $p = 0.065$, $\eta^2 = 0.03$).

There were no interactions between the factors and post-scenario attitudes (all ps>0.18), but there did seem to be a cumulative effect, such that the combination of high compulsion and centralised database led to the highest anti-ID card attitude shift for all privacy segments. A combination of low compulsion and third party database led to the most pro-ID card attitudes for all privacy segments except 'Privacy Unconcerned' (see Figures 3 and 4 below). For this group, in the low compulsion scenario, the location of the database was irrelevant to attitudes. Only in the high compulsion scenario did attitudes polarize according to the database type. For privacy fundamentalists (see Figure 4) and privacy pragmatists, post-scenario attitudes illustrated a cumulative effect of compulsion type and database.

Fig. 3. Scenario type and post-scenario attitudes of 'Privacy Unconcerned'

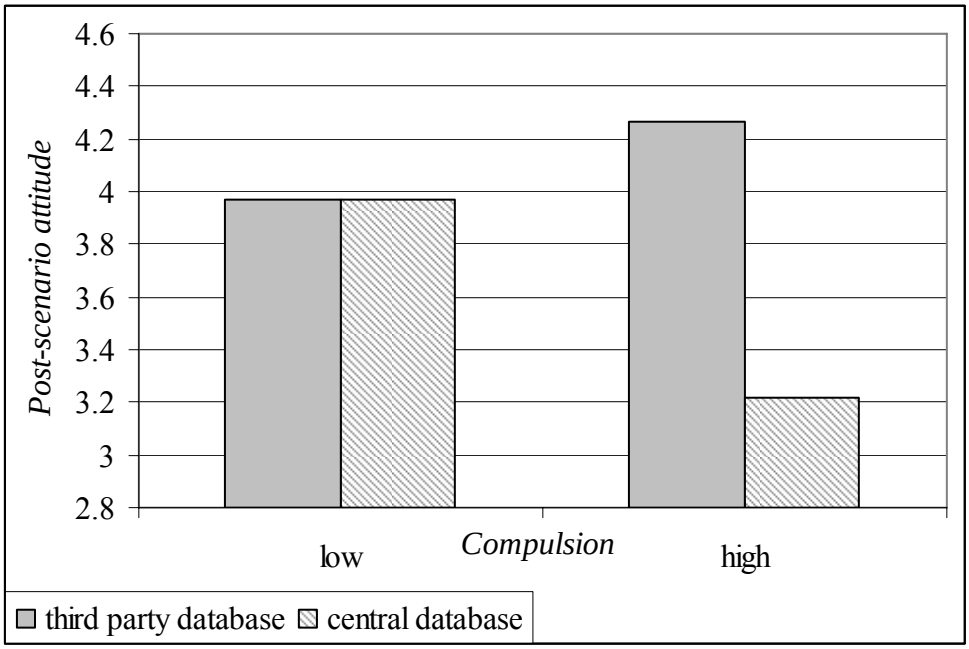
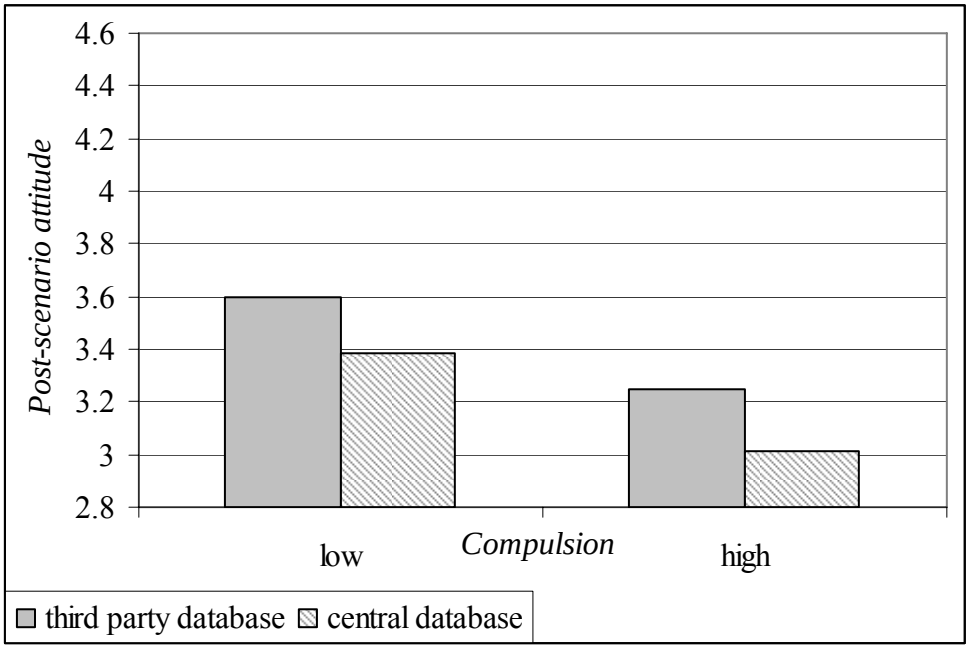


Fig.4. Scenario type and post-scenario attitudes of 'Privacy Fundamentalists'

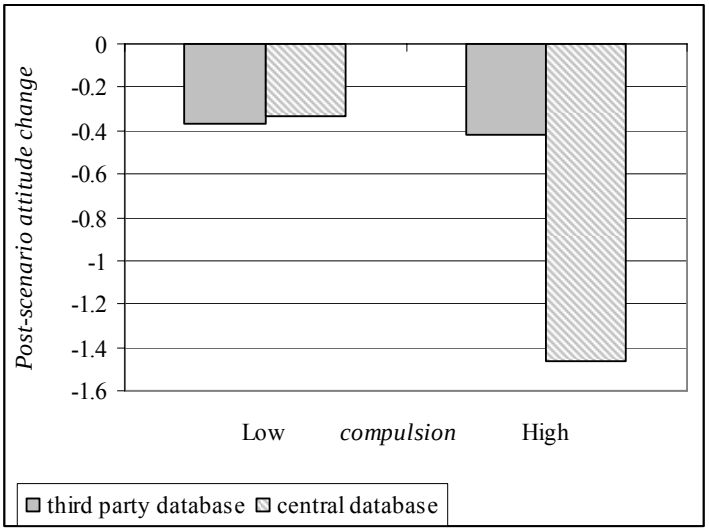


3.3. Attitude change and privacy

A further three-way ANOVA (compulsion X database type X Westin segmentation, n = 1001) was calculated to examine attitude change following the scenarios. This analysis showed statistically significant main effects of level of compulsion ($F_{(1, 988)} = 33.74$, $p<0.001$, $\eta^2 = 0.033$, high compulsion led to more negative attitude change), database type ($F_{(1, 988)} = 9.02$, $p<0.01$, $\eta^2 = 0.009$, centralised database led to more negative attitude change) but not for privacy attitudes ($F_{(2, 998)} = 0.12$, $p = 0.9$). The interaction between compulsion and database type approached statistical significance ($F_{(1, 998)} = 3.18$, $p = 0.07$, $\eta^2 = 0.003$) such that the largest attitude change was when high compulsion was combined with centralised database.

While the interaction between the scenario factors and Westin segmentation was not statistically significant ($F_{(2, 998)} = 1.9$, $p = 0.15$), there was a suggestion that the interaction between compulsion and database type outlined above was primarily due to the responses of the 'Privacy Unconcerned' – examination of the means for this group strongly suggested that the database type had no impact on attitude change when compulsion was low.

Fig.5. Scenario type and post-scenario attitude change (Privacy unconcerned)



When compulsion was high, the centralised database had the highest level of attitude change (against ID cards). For 'Privacy Pragmatists' and 'Fundamentalists', there was little evidence of an interaction – both compulsion and database type had independent effects on attitude change.

4. Discussion

Regardless of the scenario proposed in the present study, attitudes towards ID cards became more negative. The strongest impact on attitudes was when the scenario incorporated high levels of compulsion along with a centralised database. The scenario proposed in the LSE consultation document led to the least negative attitudes towards ID Cards. There is, therefore, little evidence to suggest that the UK Government's approach benefits from greater public trust as claimed [21]. The main effect of database type also suggests that the impact of a centralised database operates quite separately from the level of compulsion. Furthermore, the interaction between compulsion and database type approached statistical significance, such that the largest attitude shift against I.D. Cards was when high compulsion was combined with centralised database.

The centralised database scenarios led to more negative attitude change than the third party database scenarios. This finding also does not provide support for the government proposal of a centralised approach. Rather, it provides support for the LSE proposal of a more distributed approach, with the use of a third party store to back-up information held on the card itself. While many privacy enhancing technologies rely on the use of trusted third parties, the acceptability of such techniques amongst the general population for critical personal information is

not known. The results of the present study suggest that potential users of an Identity Card are aware of the potential security risks of a centralised database, and find a distributed approach more acceptable. In part, this may be due to an increased awareness of the potential risks involved in centralised databases – for instance, Jerry Fishenden, Microsoft UK National Technology Officer wrote in 'The Scotsman' newspaper [6] that a centralised database will create a 'honeypot' for hackers, and lead to the potential for massive identity fraud. At the time of the study, the anti-ID campaign was also running press advertisements stressing the dangers of the National Identity Register.

The high compulsion scenarios also led to more negative attitude change than the low compulsion scenarios. This finding supports the higher level of control over the type of information collected, and how and when it is collected, as proposed in the LSE blueprint, and suggested in the literature [14]. This increased control may assist in establishing trust, and a sense of autonomy and ownership over the choice of biometric data used for authentication purposes.

There was some indicative evidence that the 'Privacy Unconcerned' responded differently to the scenarios than other privacy-related segments – when compulsion was low, the 'Unconcerned' were not particularly influenced by the database type. Once compulsion was high, a centralised database led to more negative attitude change and more negative attitudes overall.

The 'Privacy Pragmatists' and 'Privacy Fundamentalists' showed no evidence of an interaction between compulsion and database type, suggesting a quantitative reaction to the scenarios, rather than the more qualitative response seen in the 'Privacy Unconcerned'. This supports Westin's view of 'Privacy Pragmatists' as weighing up privacy threats on a case-by-case, cost-benefit basis [26], although those classified as 'Privacy Fundamentalists' responded in a similar manner, albeit with more negative attitudes.

The results of the present study suggest that people's pre-existing privacy attitudes influence their reaction to possible implementation scenarios – with the 'Privacy Unconcerned' reaching a 'trigger point' of high compulsion combined with a centralised database, and privacy 'Pragmatists' and 'Fundamentalists' applying a quantitative, summative approach to the evaluation of the scenarios. This supports other work that has suggested that the adoption of smart card technologies may be influenced by people's privacy concerns and the transparency of any privacy threats posed [13]. It should also be noted that the Westin methodology for the study of privacy attitudes is not without critics [see 27], although this is partially because of the use of the term 'fundamentalist' to describe people who may simply be better informed and making reasoned decisions [27, 28], and because of tendency for his surveys to be sponsored by businesses with an interest in the use of consumer information [27]. The present research suggests that, these concerns aside, the Westin segmentation approach can provide useful insights into people's responses to different privacy threats, although our own work suggests that its focus on information privacy represents only one aspect of privacy concern [29].

In the present study, across all privacy segments, the combination of high compulsion and a centralised database caused considerable concern: in the case of privacy 'Pragmatists' and 'Fundamentalists', because of the cumulative effect, and in case of the 'Unconcerned' because of a qualitative shift in their attitudes towards ID Cards. This suggests that people with differing pre-existing privacy concerns apply different strategies to interpreting possible threats to their privacy. Those with a degree of concern may tend to adopt a summative, quantitative approach, treating elements of a proposal as individual units, while the 'Unconcerned' perhaps reach a tipping point where, in this case, high compulsion combined with a centralised database, causes a qualitative shift in attitudes.

5. Acknowledgements

This research was supported by funding from the UK Economic and Social Research Council E-Society Programme (RES-341-25-0011). We are indebted to the invaluable comments of four anonymous reviewers, and John Richardson for their comments on earlier drafts of this work.

6. References

[1] L.S.Strickland, L.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,* 56 (2004) 221-234

[2] No2ID (2005) Available at: http://www.no2id.co.uk/ (accessed June 20 2005)

[3] The Guardian, *ID cards bill faces tough time in Lords after battering from critics* (2005, October31st). Available at http://www.guardian.co.uk/guardianpolitics/story/0,,1605141,00.html (accessed October 31 2005).

[4] P.6, Should we be compelled to have identity cards? Justifications for the legal enforcement of obligations, *Political Studies*, 53 (2005) 243-261.

[5] The Office of the Information Commisioner (2005). The Identity Cards Bill: The Information Commissioners Concerns. Available at: http://www.ico.gov.uk/cms/DocumentUploads/the_identity_cards_bill_ico_concerns_october_2005.pdf (Accessed November 2nd, 2005)

[6] J. Fishenden, *ID cards will lead to 'massive fraud'* (2005). Available at: http://news.scotsman.com/index.cfm?id=2103982005 (accessed 18 October 2005).

[7] Home Office (2005). Identity Cards: An assessment of awareness and demand for the Identity Card Scheme. Available at: http://www.identitycards.gov.uk/library/2005-10-12_Trade_Off_final_report.pdf (Accessed 2nd November 2005)

[8] M.J.Metzger, *Privacy, trust and disclosure: Exploring barriers to electronic commerce* (2004). Available at http://jcmc.indiana.edu/vol9/issue4/metzger.html (accessed 20 June 2005).

[9] J.Nickel and H.Schaumburg, *Privacy, trust and self-disclosure in e-recruitment*. Paper presented at CHI, Vienna, Austria 24-29 April 2004

[10] J.Phelps, G.Novak and E.Ferrell, Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing* 19 (2000) 27-41.

[11] D.A.Taylor and I.Altman, Self-Disclosure as a Function of Reward-Cost Outcomes. *Sociometry*, 38 (1975) 18-31.

[12] T.B.White, Consumer disclosure and disclosure avoidance: a motivational framework. *Journal of Consumer Psychology* (2004) 14, 41-51.

[13] S.G.M. Bailey and N. Caidi, How much is too little? Privacy and smart cards in Hong Kong and Ontario, *Journal of Information Science*, 31 (2005) 354-364

[14] M.J. Culnan and P.K.Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation, *Organization Science*, 10 (1999) 104-115.

[15] J.Oates, *Internet worries US consumers* (2005). Available at http://www.theregister.co.uk/2005/10/18/survey_fears/ (accessed 18 October 2005)

[16] Harris and Associates Inc. and A.Westin, E-*commerce and privacy: What net users want, Privacy and American Business and Pricewaterhouse Coopers LLP* (1998). Available at: http://www.pandan.org/ecommercesurvey.html (accessed 20 June 2005).

[17] Computerworld. Available online at: http://www.computerworld.com/printthis/2005/0,4814,101766,00.html (accessed 4th November 2005).

[18] The Times, Cost of ID cards 'may spiral to £300' (2005, June 16th) Available at http://www.timesonline.co.uk/newspaper/0,,173-1656121,00.htm (accessed July 5 2005).

[19] LSE, *Alternative blueprint for a national identification system* (2005). Available at: http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/LSE_ID_blueprint.pdf (accessed 5 July 2005)

[20] Home Office, Home Office response to the London School of Economics' ID cards cost estimates and alternative (2005). Available at:

http://www.identitycards.gov.uk/library/Response_LSE_Alternative_Blueprint.pdf (accessed November 2nd 2005)

[21] Home Office, *Identity cards trade off research interim report* (2005). Available at: http://www.identitycards.gov.uk/library/2005-06-27_Identity_Cards_Trade_Off_Research-Interim_Report_v1.0.pdf (accessed November 2nd 2005)

[22] C.Bellamy, P.6, and C. Raab, Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part II, *Public Administration*, 83 (2005) 393-415.

[23] A.Westin Consumers, privacy and survey research. Paper presented at CASRO, Las Vegas, October 2003. Available at: http://www.harrisinteractive.com/advantages/pubs/DNC_AlanWestinConsumersPrivacyandSurveyResearch.pdf (accessed July 5 2005).

[24] A. F. Westin. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, Volume 59, Number 2, pp. 431-453(23)

[25] H.Taylor, Most people are 'Privacy Pragmatists' who, while concerned about Privacy, will sometimes trade it off for other benefits, *The Harris Poll*, March (2003). Available at http://www.harrisinteractive.com/harris_poll/index.asp?PID=365 (accessed July 5 2005).

[26] Privacy Knowledge Base (2005). Available at http://privacyknowledgebase.com (accessed June 20 2005).

[27] Electronic Privacy Information Centre, Public Opinion and Privacy (2005). Available at http://www.epic.org/privacy/survey/default.html (accessed December 1st, 2005)

[28] Oscar H. Gandy, Jr. The role of theory in the policy process. A response to Professor Westin. In: C. Firestone and J. Schement (eds.), *Toward an Information Bill of Rights and Responsibilities*, (Washington DC: The Aspen Institute Communications and Society Program, 1995).

[29] Paine, C., Reips, U-D., Steiger, S., Joinson, A.N., and Buchanan, T. *Internet users' perceptions of 'privacy concerns' and 'privacy actions'*. (Unpublished manuscript, Open University, Milton Keynes, 2005)