Privacy Concerns, Trust in Government and Attitudes to Identity Cards in the United Kingdom

Adam N. Joinson
School of Management, University of Bath
A.Joinson@bath.ac.uk

Abstract
In the present paper, the links between privacy concerns, trust in the Government and compulsion are examined in light of people’s attitudes towards Identity Cards in the United Kingdom. A total of 404 respondents from both politically active and student groups were presented with scenarios for the implementation of ID Cards in which the degree of compulsion was varied. Their levels of privacy concern about ID Cards and trust in the Government were also measured. The perceived degree of compulsion, privacy concerns and trust in the Government predicted attitudes to Identity Cards. Mediation and moderation analyses were conducted to examine the relationship between privacy, trust and ID Card attitudes. It was found that the impact of privacy concern on attitudes was moderated by trust, such that amongst respondents with lower privacy concerns, lack of trust moderated this to lead to negative attitudes towards Identity Cards. Implications are discussed.

1. Introduction
E-government initiatives tend to impose a privacy cost on citizens, whether through data sharing between Government departments, requests for (or the collection of) personal and identifying information, and the requirement for the storage of that same data [24, 47]. This led [29] to note that a “critical obstacle in realizing e-government is the citizens’ concern on privacy of their life and confidentiality of the personal data they are providing as part of obtaining government services” (p. 134). Compared to the use of e-commerce, e-government also often demands information from citizens rather than requests it [47], a compulsion that may make any privacy violation particularly difficult to manage [28].

The relationship between people’s privacy concerns and their willingness to accept (or reject) privacy threatening technologies is neither straightforward nor well understood [1, 28, 34]. There are multiple studies to suggest that reported privacy concerns rarely lead people to take privacy protecting action [1, 35, 41]. However, individuals may take privacy into account when the nature of the activity is particularly sensitive (e.g. purchasing condoms rather than a book; [21]), or when they have high privacy ‘self-efficacy’ [30]. Within the realm of e-government, cultural differences in privacy concern and trust in government have also been identified as key issues in determining acceptance [4, 15, 38].

A key variable identified in e-commerce research as critical to understanding the link between privacy concerns and behavior is trust [8, 14, 16, 32, 35, 37]. Trust can be defined as, “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” (p. 712) [33]. Put more simply, it is the “willingness to be vulnerable, based on positive expectations about the actions of others” ([10].p.1). Trust incorporates a number of different dimensions [8], including the trustee’s ability to fulfill the trusting action, their integrity, and the benevolence of their intentions.

In terms of e-government, trust has also been identified as critical in the acceptance of potentially privacy violating technologies [12, 13, 44, 47]. In cases where trustworthiness is in question, acceptance levels may reduce. For instance, 11% of Icelandic citizens opted out the country’s DNA database after government attempts to sell access to commercial researchers [3]. The United Kingdom National Audit Office [36] reports that, although the implementation of e-government in vehicle licensing was successful, it may “need to revisit its conclusions in light of the impact of recent data protection failures on customer usage and costs”. This concern echoes earlier reports by the US GAO [20] on e-government that note the importance of providing secure transactions, protecting consumer privacy and enabling trust.

While the role of trust in determining people’s willingness to forgo privacy concerns has been reasonably well established [16, 32, 37], the exact
nature of the relationship between privacy, trust and behavior hypothesized by researchers tends to vary. Most commonly, trust is predicted to mediate the link between privacy concerns and behavior \cite{34, 32, 37} In its traditional sense, mediation refers to the effect of an independent variable on a dependent variable being explained by common links to a third variable (i.e. the mediator) \cite{6}. For instance, a correlation between income and cancer might be explained by a correlation between income and smoking (the mediator), and then between smoking and cancer. Thus, according to mediation models, privacy has little or no direct effect on behavior (path a in Figure 1), instead any effect can be explained by the links between privacy and trust (path b), and then between trust and behavior (path c).

![Figure 1: Privacy Trust Mediation](image)

An alternative approach towards understanding the relationship between related variables is moderation \cite{6}. Moderation is when the impact of a variable on an outcome measure (for instance, vitamin supplements on health) is altered by the status of a moderator (e.g. vitamin plus precondition leads to negative outcome, absence of precondition leads to positive outcomes). In the case of privacy and trust, it may be that the effect of privacy on behavior is moderated by trust, such that in conditions of high trust, privacy concern exerts an influence on behavior, while in low trust environments privacy concern may have a negligible impact on behavior since behavior is limited by trust concerns. In the present study, mediator and moderator relationships between privacy concerns, trust in Government and attitudes towards Identity Cards are studied.

1.1 Identity Cards

A critical component of e-government is the identification and authentication of citizens to Government agencies \cite{13, 14}. In many countries this is achieved through the provision and use of a single identifier (e.g. identity card or social security number), which increasingly poses dangers for citizens in terms of identity theft and fraud \cite{22, 31}. Many Western countries without a form of identity card (e.g. the United States, United Kingdom, Australia) have taken steps towards either the introduction of a specific identity card (in the case of the UK), or the standardization of identity documents across States (e.g. REAL ID in the USA). The focus of the present paper is the introduction of an Identity Card and related database in the United Kingdom.

The possibility of identity cards was first proposed by the current UK Government in 2002 as an ‘entitlement card’ (i.e. to prove one’s identity in order to claim healthcare and other benefits). This proposal became an ‘Identity Card’ that was included in the manifesto of the Labour Party in the 2005 election. Following their re-election, the Identity Card Bill was presented to Parliament in May 2005, and was finally passed in March 2006.

The planned UK Identity Card has been controversial for a number of reasons. First, the implementation method chosen requires a centralized database (called the ‘National Identity Register’ or NIR) against which identity claims and biometrics are compared. Alongside biometrics, the NIR will also contain up to 51 pieces of information about an individual, including current and past addresses. Each time the National Identity Register is queried, a log of the request is stored on the system, posing a possible privacy threat through the accumulation of ‘data footprints’ \cite{25}. Moreover, the use of a centralized database to manage the NIR has led to a number of security-based concerns (e.g. \cite{19}), as well as the possibility that it will be a ‘choke point’ for requests or a target for denial of service attacks \cite{22}. Second, it has been claimed that the plans of the UK Government lack clear well-defined goals \cite{31, 49}. For instance, during the passage of the legislation, the introduction of ID Cards was claimed to tackle identity theft and terrorism, but in neither case were the reasons for these claims explicated \cite{49}. Finally, it has been argued that the costs of the scheme were grossly underestimated by the UK Government \cite{31}.

The introduction of Identity Cards in the UK has also raised concerns amongst civil liberty, privacy and data-protection groups (see http://www.no2id.net). Indeed, public acceptance of Identity Cards has been reducing, from approximately 75% of the population in favor in 2004 to around 50% in 2007.

1.2 Compulsion and Identity Cards

The manifesto pledge by the Labour Party in 2005 was that ID Cards would be voluntary. However, the Identity Card Bill as presented by the UK Government legislated that there would be no such opt-out, and that
people would be required to have an ID Card when applying for a passport (the argument being that choice came through whether or not to apply for a passport).

At the time of the present research, the ID Card Bill was subject to an amendment focused on whether or not the ID Card, and entry of personal details to the proposed National Identity Register (NIR), would be voluntary or compulsory. The specific amendment proposed by the House of Lords sought to enable people to opt-out of an ID Card when applying for a new passport or renewing an existing passport.

Within the literature on privacy and data protection, consumer and citizen control and choice is critical [16]. For instance, the UK Data Protection Act (1998) requires that data subjects are informed that data is collected, and given the choice as to whether or not to provide their information. [17] reports to the FTC that privacy policies should incorporate informed consent from data subjects. In terms of e-government and interactions between citizens and state, issues of choice are muddied. In many cases the state may require (or demand) information (e.g. tax returns, census data), and may punish those who do not comply. Similarly, in terms of proving one’s entitlement to state aid (e.g. healthcare, unemployment benefits, tax credits or refunds), non-compliance exerts a direct cost on individuals in terms of non-provision of goods or services.

However, in most cases this degree of compulsion is accepted by citizens because there is a clear need for the information, or a clear public good [18, 42]. In the case of ID cards, given the lack of clarity of goals for their introduction [31], it is perhaps not surprising that the issue of choice became central to arguments about their implementation.

The aim of the present study was two-fold. The first was to examine the impact of choice and compulsion on attitudes towards Identity Cards in the UK. The second was to examine the impact of privacy concerns and trust in the Government on attitudes towards Identity Cards. Two populations are studied – politically active Internet users and mature students – in order to examine if the same pattern of relationships between privacy concerns, trust, control and attitudes exist in diverse groups.

2. Research Study
2.1 Participants

Participants were recruited from a number of sources. The politically active participants were recruited through postings on three UK politics discussion groups: uk.politics, uk.politics.id-cards and on the ‘Westminster’ forum of http://www.politicsforum.co.uk. Postings on general Open University UK student discussion boards were used to recruit the student participants. The Open University is a large distance education higher education institution with a diverse student body. Given the nature of the recruitment, response rate information is not available. Level of political involvement was inferred from group membership, although of course this does not rule out the possibility that some student group members were also politically active.

In all cases, participants were directed to an online survey hosted by the Open University online survey system (called ELSA). The front page of the survey randomly assigned participants using JavaScript to one of three conditions, (1) HIGH COMPULSION (2) LOW COMPULSION (3) LOW COMPULSION with CONTROL. These conditions approximated the implementation of Identity Cards as proposed by the UK Government (1), the Lords’ amendment (2), and the London School of Economics (3). The design of the study materials and experimental manipulations is shown in Figure 2.

![Figure 2: Experimental design](image)

An alternative procedure (season of birth) was automatically used if people did not have JavaScript enabled on their browser. The ELSA system also sets a session-based cookie to help track multiple sessions, and records the IP number associated with each submission to identify multiple submissions.
The data collected was cleaned in a number of ways. First, any responses with less than 50% of items answered were discarded. Second, the server log files were examined for instances of multiple submission. There were no cases of multiple submissions with the same session based cookie. There were 39 instances where a response shared an IP with another response. Examination of these responses showed that in 37 cases, the IP belonged to the proxy or cache server of a large UK-based Internet Service Provider. In 8 cases, the shared IP was identified as belonging to different people because one record originated from an internal Open University posting, and the second from a public posting. In these cases the data was retained. In the remaining 31 cases, the data was discarded from the analyses.

2.1.1 Participants

There were 181 responses from the postings to the three politics groups. Of these, 137 (75.7% were male) and 41 female (22.5%). Demographic data was missing for three people. The mean age of the sample was 36 years (SD = 12.92).

There were 223 responses from the postings to Open University student tutorial groups. Of these, 66 were male (29.6%) and 156 female (70%), and data was missing for 1 respondent. The mean age was 39 years old (SD = 11.49).

3. Measures

3.1 Pre-manipulation Identity Card attitudes

Participants were first 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 (1) ‘Strongly against ID cards” and (7) ‘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 (7) ‘Very certain” and (1) ‘Very uncertain’). Participants who are not UK citizens, or who do not live in the UK, were excluded from any analyses of ID card attitudes (n = 6).

3.2 Implementation of Identity Cards

Participants were instructed that:

*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.*

An implementation scenario then followed the introduction. The scenario proposed varied across a single dimension based on differing options proposed by the UK Government, the Lords’ amendment and the LSE. Each scenario was pre-tested for ease of understanding, and matched for word-count. The scenarios were based on those used in previous research [27]. The component parts of the scenarios were:

**UK Government (UKG):**

*When you apply for a new or renewed passport, you will be compelled to also have an Identity Card. You will be told to report with existing documents (e.g. birth certificate, old 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.*

**Lords’ Amendment:**

*When you apply for a new or renewed passport, you will be given the choice of whether or not to also have an Identity Card. If you choose to also apply for an Identity Card, you will be told to report with existing documents (e.g. birth certificate, old 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.*

**London School of Economics (LSE):**

*When you apply for a new or renewed passport, you will be given the choice of whether or not to also have an Identity Card. 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.*

In all three cases, the National Identity Register (NIR) as proposed by the Government was also included in the scenario. The wording was identical in the Lords and LSE scenarios, and the ‘If you choose to have an ID card’ part was omitted in the UK Government version.
National Identity Register part of scenarios:
If you choose to have an ID card, your 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 centralized 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 organizations (e.g. banks, employers).

When participants accessed the front page of the study (which contained basic information and contact details about the researchers), they were randomly directed to one of the three different scenarios. 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 favor of ID cards. Participants were also asked, “In this scenario, to what extent would you consider yourself to have been forced to comply to receive an identity card?” This question was answered using a 7-point scale anchored at ‘Not at all forced’ and ‘Very forced’.

On the final page of the study, participants completed a short measure to test their privacy attitudes [27], their trust in the UK Government, (three questions, see below) and the perceived threat to their privacy of the ID Card proposals (two questions, see below).

3.3 Trust in the UK Government

Participants completed three questions: “The United Kingdom Government can be trusted”; “The United Kingdom Government is competent enough to create a secure Identity Card system”, and “The United Kingdom Government is motivated by the desire to protect its citizen’s best interests” using a 4 point scale anchored at ‘Strongly Agree’, ‘Somewhat Agree’, ‘Somewhat Disagree’ and ‘Strongly Disagree’. No neutral option was provided to reduce satisficing. These items cover three dimensions often associated with the measurement of trust: general trust, competence and benevolence. The trust scale had an alpha of .82, showing acceptable internal reliability.

3.4 Perceived Privacy Threat of ID Cards

Participants also completed two items designed to measure the perceived privacy threat of ID cards: “The introduction of Identity Cards in the UK is a threat to people's personal privacy” and “Data collected as part of the Identity Card system would be treated confidentially” (Reversed) using the same 4-point Likert scale for Trust. The perceived privacy items had an alpha of .60, showing low but acceptable internal reliability for a two item scale.

As would be expected, the privacy and trust scales were correlated (r = .71, p < .001). Confirmatory factor analysis using principal axis factoring with a forced two factor solution and Oblimin rotation supported the creation of two scales.

4. Results and Discussion

A manipulation check was conducted to see if the level of perceived compulsion differed across scenarios. There was a main effect of scenario on perceived compulsion (F (2, 390) = 31.2, p < .000). Post hoc Scheffe tests confirmed that the UKG implementation led to higher perceived compulsion scores (Mean = 5.99) compared to the Lords’ amendment version (Mean = 4.56, p < .001), and the LSE version (Mean = 4.01, p < .001). The Lords’ and LSE scenarios did not differ significantly in their level of perceived compulsion (p=.25).

4.1 Politics and OU groups – general attitudes

The initial attitudes of the politics and student groups differed significantly in both their attitudes towards ID Cards, the certainty with which they held those attitudes, their trust in the UK Government, the perceived privacy violation posed by ID Card proposals, and their general privacy concerns (see Table 1)

Participants in the politics groups were more anti-ID Cards, held these attitudes with greater certainty, distrusted the government more, perceived ID cards as a greater threat to privacy, and had greater general privacy concerns. However, even amongst OU students, who on average were in favor of ID cards, levels of distrust in the UK Government and the perceived privacy threat of ID cards were still relatively high.
Table 1: Politics versus OU Students: general attitudes (Mean, SD) and one-way ANOVA results

<table>
<thead>
<tr>
<th>Measure</th>
<th>Group</th>
<th>F (df=1, 385)</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-scenario attitudes to ID Cards</td>
<td>Politics (Mean, SD)</td>
<td>1.62 (1.34)</td>
<td>3.99 (2.16)</td>
</tr>
<tr>
<td></td>
<td>Open University (Mean, SD)</td>
<td>5.22 (1.87)</td>
<td>37.07</td>
</tr>
<tr>
<td>Pre-scenario certainty of attitudes</td>
<td>Politics (Mean, SD)</td>
<td>6.27 (1.50)</td>
<td>5.22 (1.87)</td>
</tr>
<tr>
<td></td>
<td>Open University (Mean, SD)</td>
<td>3.05 (0.70)</td>
<td>84.60</td>
</tr>
<tr>
<td>Distrust in UK Government</td>
<td>Politics (Mean, SD)</td>
<td>3.64 (0.53)</td>
<td>2.99 (0.80)</td>
</tr>
<tr>
<td></td>
<td>Open University (Mean, SD)</td>
<td>2.78 (0.55)</td>
<td>7.86</td>
</tr>
<tr>
<td>Privacy threat of ID Card proposals</td>
<td>Politics (Mean, SD)</td>
<td>3.66 (0.59)</td>
<td>2.78 (0.55)</td>
</tr>
<tr>
<td></td>
<td>Open University (Mean, SD)</td>
<td>2.78 (0.55)</td>
<td>7.86</td>
</tr>
<tr>
<td>Westin-Harris Privacy score</td>
<td>Politics (Mean, SD)</td>
<td>2.94 (0.59)</td>
<td>2.78 (0.55)</td>
</tr>
</tbody>
</table>

4.2 Attitude change

A measure of attitude change was calculated by subtracting post-scenario attitudes from pre-scenario attitudes. The average ID Card attitude change was negative (Mean = -.41, SD = 1.23), indicating a move against ID cards across all three scenarios.

4.2.1. Scenarios and attitude change

In the following analyses, the responses of the politics participants and the OU students are analyzed separately.

The presentation of different implementation scenarios did not have a significant effect on attitude change (F (2, 214) = 1.20, p = .31) or the certainty of the later attitude (F (2, 213) = .19, p = .82) amongst the student participants.

The presentation of different implementation scenarios also did not have a significant effect on attitude change for the politics groups (F (2,172) = .97, p = .38). Interestingly, attitude change towards ID cards was positive when the LSE scenario was presented (the only positive shift in any condition).

However, the scenario presented did have an impact on the certainty of the later attitude (F (2, 172) = 3.20, p = .04). Members of the politics groups were less certain of their attitude when faced with the LSE approach (Mean = 5.95, SD=1.83), compared to the Lords’ amendment (Mean = 6.46, SD=1.36) and the UK Government approach (Mean = 6.62, SD=1.29).

4.3. Trust in Government, privacy attitudes and ID Cards

As noted earlier, the two groups of participants had differing attitudes towards the Government, ID cards and general levels of privacy concern. A linear multiple regression was calculated in order to examine the impact of the perceived privacy threat of ID cards, general privacy concerns and levels of trust in the government on respondents’ post-scenario attitudes. A regression was first calculated to examine the impact of age, gender and source (politics groups vs. students) on post-scenario attitudes. Age and gender were not significant, but source did significantly predict post-scenario attitudes (β = .40, p<.001). As such, the source of the participants (political groups vs. students), and their pre-scenario attitudes were entered into the regression equation as control variables. The results of the analyses are shown in Table 2.

Table 2: Multiple regression: Dependent variable: Post-scenario attitude toward ID Cards (R² = .75, p<.000)

<table>
<thead>
<tr>
<th>Variable</th>
<th>β</th>
<th>t</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Politics vs. Students</td>
<td>-.01</td>
<td>-1.18</td>
<td>.86</td>
</tr>
<tr>
<td>Pre-scenario attitudes</td>
<td>.51</td>
<td>10.69</td>
<td>.00</td>
</tr>
<tr>
<td>Pre-scenario attitude certainty</td>
<td>.06</td>
<td>2.20</td>
<td>.03</td>
</tr>
<tr>
<td>Presented scenario</td>
<td>-.02</td>
<td>-6.9</td>
<td>.49</td>
</tr>
<tr>
<td>Perceived compulsion in scenario</td>
<td>-.14</td>
<td>-10.1</td>
<td>.00</td>
</tr>
<tr>
<td>Distrust in Government</td>
<td>-.11</td>
<td>-2.67</td>
<td>.01</td>
</tr>
<tr>
<td>Perceived privacy threat of ID cards</td>
<td>-.26</td>
<td>-5.65</td>
<td>.00</td>
</tr>
<tr>
<td>Mean Westin Score</td>
<td>.01</td>
<td>3.2</td>
<td>.75</td>
</tr>
</tbody>
</table>
towards ID Cards was the perceived privacy threat of the ID Card proposals, followed by the perceived degree of compulsion involved in ID Cards. As reported earlier, the UKG approach was seen as involving the highest amount of compulsion, although given that scenario type was not significant, we should also assume an affective component to this evaluation alongside the content of the scenarios. Third, the level of distrust in the UKG also predicted post-scenario attitudes to ID Cards, such that higher levels of distrust led to more negative attitudes. Finally, the certainty with which pre-scenario attitudes were held also predicted post-scenario attitudes – if pre-scenario attitudes were less certain, this led to more negative attitudes after the scenario was presented.

The results of the regression strongly suggest that privacy concerns associated with ID Cards, distrust of Government and perceived compulsion of the implementation, significantly predict people’s attitudes towards ID Cards. These results are in keeping with considerable research within the Human-Computer Interaction and e-commerce fields that have highlighted the importance of trust in people’s response to privacy threats. That perceived compulsion was also a significant predictor, while scenario type was not, strongly suggests an affective element to ‘control’ (as best expressed by the LSE scenario).

4.4: Privacy, Trust and Attitudes to ID Cards

The mediation of perceived privacy threat by trust on attitudes towards Identity Cards was tested using a series of regression equations [6].

The moderation analyses show that while citizen’s privacy concerns and trust have a direct impact on attitudes towards the implementation of Identity Cards in the UK, there is also an interaction between privacy and trust.

To examine the nature of this interaction in more detail, the privacy and trust variables were median split into high and low trust and privacy concern, and a two-way, between-subjects ANOVA conducted. The interaction between privacy and trust was significant ($F(1, 386) = 26.60, p<0.00$. The pattern of this interaction is illustrated in Figure 5.

The interaction suggests that for those who considered ID Cards to be a threat, level of trust in the Government had little impact on their attitudes. However, for those who were more ambivalent about the privacy threat of ID Cards,
the level of trust was critical in determining their attitudes. Specifically, in this group low levels of trust led to negative attitudes towards ID Cards, and high levels of trust led to more benign, positive attitudes.

According to the UK Information Commissioner, the United Kingdom faces the prospect of ‘sleepwalking into a surveillance society’ [5]. In terms of e-government, citizen privacy concerns pose a substantial obstacle towards the implementation of data sharing, identity management schemes and verifiable authentication [7, 15, 38, 39, 42]. The results of the present study provide a number of important and novel insights into people’s privacy concerns and their attitudes towards the implementation of Identity Cards in the UK. First, although the different methods of implementation did not differ significantly in terms of attitude change, they did have an impact on citizens’ perceived compulsion. This suggests that issues of control and compulsion have an affective component, as well as one as outlined in systems design. This is important since the affective component is likely to be influenced by people’s ‘sense’ of control and compulsion, rather than their actual level of control. Successful e-government initiatives should seek to not only provide control to citizens, but should also make them feel in control.

The relationship between the perceived privacy threat of ID cards and opposition to them was strong, suggesting that e-government initiatives that collect data on citizens may encounter considerable opposition if the data collection is perceived as impinging on personal privacy. This was supported by both the regression analyses and the ANOVA. When there was a high perceived privacy threat, levels of trust did not moderate attitudes towards ID Cards. Only when the perceived privacy threat was felt less keenly by participants did trust impact on their attitudes towards ID Cards.

This finding is important since we usually assume that ‘privacy fundamentalists’ will generally oppose any e-government system that poses a privacy threat, and the ‘privacy unconcerned’ perhaps won’t worry regardless [27]. However, ‘privacy pragmatists’ are likely to judge a particular system in light of not only its costs and benefits, but also in relation to the potential data collector. The evidence in favour of moderation suggests that combining privacy threat with low levels of trust creates a particular impetus towards opposition – something that may swing pragmatists towards opposition [27].

5.1 Implications for e-government

As noted, once e-government systems are developed beyond information portals, there is an increased need for the collection of personal information, data sharing between departments and databases, and authentication of individuals and their entitlements. There are a number of methods available to develop e-government in a ‘privacy friendly’ way (e.g. through trusted third parties or identity management systems). The results of the present research strongly suggest that the developers of e-government ignore issues of privacy at their peril. In particular, trust would seem to be the keystone in terms of building e-government systems that request or reuse personal information. This trust can take the form of competence (e.g. in the development of systems or the protection of personal information), or in the integrity of the Government itself. However, the absence of trust is likely to render even privacy-friendly e-government initiatives unsuccessful.

5.2 Implications for privacy and trust research

Privacy has been described as a ‘concept in disarray’ [40]. In part this is due to one of the strengths of the research area – its multi-disciplinary nature – but also because privacy can refer to so many different contexts and meanings [28]. The research presented here strongly suggests that the interaction between privacy concern and trust is critical to understanding people’s responses to a potential privacy threat. Specifically, the creation and testing of the multiplicative composite provided strong evidence that the combination of low trust with privacy threat leads to a stronger reaction than would be expected by examining just privacy and trust independently.

Theoretically, there are good reasons to assume that the combination of low trust with privacy threat poses a unique threat to people’s acceptance of a
technology. For instance, Altman [2] describes a self boundary (the boundary around the person) that is modified by the disclosure of personal information; and a dyadic boundary that ensures the discloser’s safety from leakage of information to uninvited third parties. The self boundary may be open or closed depending on such interpersonal factors as the level of trust in a disclosure target.

In the present research, the combination of privacy concerns and low trust may have replicated a situation in which the self boundary is open (i.e. information is recognized as at risk), but the impermeability of the dyadic boundary is open to question (i.e. information may be leaked to a third party or misused). This analysis suggests the possible benefits of applying insights from interpersonal interaction to the interactions between citizens and governments – if, as suggested by some, we are moving towards an era of personalized e-government [23], then there are clear privacy implications [14, 45], alongside the need to consider issues of trust in terms of citizen-state interactions [11].

5.3 Limitations and future research

In the present research, a single aspect – identification and authentication - of citizens’ relations with the state were studied. The case of ID Cards poses a number of issues in terms of generalizability that will need to be tested. First, the potential costs and benefits of ID cards in the UK are hotly contested, suggesting that not all respondents’ conceptions of the scenarios were similar. The importance of each individual’s own interpretation was seen in the non-significance of the compulsion scenarios, and the importance of perceived compulsion, on attitudes towards ID Cards. Given that at the time of the research the legislation was being discussed in depth in the UK media, perhaps it is not surprising that people came to the study with pre-existing attitudes that were stronger than the manipulated scenarios.

6. References