Federated Identity to Access e-Government Services – Are Citizens Ready for This?

Sacha Brostoff
Information Security Research Group (ISRG)
Dept. of Computer Science, University College London, UK
s.brostoff@ucl.ac.uk

Charlene Jennett
ISRG, Department of Computer Science
University College London, UK
c.jennett@ucl.ac.uk

Miguel Malheiros
ISRG, Department of Computer Science
University College London, UK
m.malheiros@ucl.ac.uk

M. Angela Sasse
ISRG, Department of Computer Science
University College London, UK
a.sasse@ucl.ac.uk

ABSTRACT
Both the US & UK government have decided that citizens will to authenticate to government using Federated Identity (FedID) solutions: governments do not want to be Identity providers (IdPs), but leverage accounts that citizens have with other service providers instead. We investigated how citizens react to their first encounter FedID authentication in this context. We performed 2 studies using low fidelity prototypes with: in study 1, 44 citizen participants, & in study 2, 22 small business owners, employees & agents. We recorded their reactions during their user journey authenticating with 3rd party providers they already had accounts with. In study 1, 50% of participants said they would not continue to use the system on reaching the *hub page*, & 45% believed they were being asked to make a payment. 25% of those continuing said they would stop when they reached the *consent page*, where they were asked by their IdP to authorise the release of their identifying information to the government service. 34% of the participants felt threatened rather than reassured by the privacy protection statement. With study 2's improved prototype, only 14% of participants said they would not continue on reaching the *hub page*, & 6% abandoned at the *consent page*. Our results show that usability & acceptance of FedID can be greatly improved by the application of standard HCI techniques, but trust in the ID Provider is essential. We finally report results from a survey of which ID providers UK citizens would trust, & found significant differences between age groups.

Categories and Subject Descriptors
H.1.2 [**Models and principals**]: User/Machine Systems - *Human factors*.

K.4.4 [**Computers and society**]: Electronic commerce - *Security*

General Terms
Design, Experimentation, Security, Human Factors.

Keywords
Usability; Federated Authentication; Identity Management.

1. INTRODUCTION
Most governments in industrialised nations want to move government services online, to offer citizens more convenient access, and reduce transaction costs. Both the UK and US governments have decided that those goals are best realised by using federated identity to authenticate citizens. This means that – rather than receiving a an online government identity – like citizens of Italy, Denmark and Estonia do, to name a few examples – US and UK citizens will use a Federated Identity (FedID) solution to authenticate. Basically, they will use online credentials they hold with certified third party - identity providers (IdPs) to access online services offered by relying parties – both commercial and Governmental. Instead of accessing your tax records by entering your Government issued username, PIN and password, you will access them (for example) by typing your online banking credentials into your bank's website, and be transferred to the page for your records at the Government's Tax service.

In addition to offering lower transaction costs and enhanced administrative capabilities (reducing the number of accounts and fraud),.FedID is supposed to offer security and convenience to the citizen. Eradicating the burden of multiple usernames and passwords is a focus of identity management system design [10]. The burden has been amply documented [e.g. 9], as have users' attempts to reduce the burden by using the same usernames and passwords across different accounts [6] – a risky practice. By enabling existing credentials to be used securely across a larger number of systems, federated identity systems impose less burden on the citizen to remember credentials that they are likely to use infrequently, but that are extremely important – such as tax returns. FedID should makes it less effort to access those services and less likely citizens find themselves locked out – which can lead to significant problems, e.g. when they cannot file their tax return on time. Moreover, security of the credentials is likely to be higher in services that citizens use frequently (breaches are more likely to be noticed, and sooner).

In the UK Identity Assurance (IDA) program, the Government has mandated that the system should support the following principles (among others) [1]:

- privacy for citizens when transacting,
- choice in who provides identity services, and
- transparency in the transfer and use of personal data.

These principles are desirable in identity federation system design [3], and mean that 3rd parties providing identity services for citizens should not know which relying parties they are transacting with, and vice versa. In our example, the bank you use at IdP would not know the citizen is transacting with the tax authority, who, in turn, would not know that you're logging in via your bank. Citizens not comfortable using a particular IdP for a particular transaction can choose different IdPs for different services: for example, a citizen may choose the bank as IdP for some services, and their webmail provider for others..

However, all identity management systems require users to perform "security actions" (such as presenting a security token, or entering a knowledge-based credential) based upon security conclusions (e.g. determining the security state of a system from observations, such as the presence of closed padlock icons in browser chrome) [10]. These indicators harbour usability challenges - users have to understand to notice them, understand what they mean, and chose the correct action [10]. One example in FedID is *consent*:-users must approve (or reject) the sharing of their digital credentials. In current online transactions, consent is obtained rarely according to Friedman's [8] criteria for informed consent. There are concern that FedID mechanisms could lead to unintended disclosure and privacy breaches because users do not understand what they are consenting to [5]. Other causes for accidental disclosure are that most users – focussed on their primary task – are likely to dismiss warnings, and trust what they perceive as familiar service providers and technologies [11]. While some heuristics have been proposed predicting the acceptance of national identity management systems [e.g. 13], they have not been tested with a variety of populations. We currently have insufficient knowledge to predict if a particular national user population will understand how to use FedID in the government context, and reject or embrace it. . The only widely successful FedID solution to date is *FaceBook Connect* [cf. 6], which is promoted to users as a convenience, and not designed to protect their privacy – arguably, its intention is exactly the opposite. In this paper we describe three studies that were carried out with representatives of the intended user population on prototype designs of the UK FedID solution.

Studies 1 and 2 were think-aloud laboratory usability tests of low-fidelity prototypes, with different user journeys and different groups of users. Study 3 was an online survey on acceptability of different types of IdPs. We first describe the method and results of each of the studies, discuss what they mean for answering the question posed in the title, and present our conclusion of what needs to be done to make FedID work in the government context.

2. STUDY 1: NHS USER JOURNEY

In Study 1 we tested two 'low fidelity' prototypes to illustrate a National Health Service (NHS) user journey, where participants are asked to imagine they are logging in through a Post Office account (IdP) in order to make an NHS appointment for their hospital test results. Prototype NHS 1 had a plain *hub page*. Prototype NHS 2 had a *hub page* with trust seals, social networking links and contact links and information.

2.1. Method

2.1.1.Participants

We recruited 44 particpants, who are UK resident and regularly transact online., All had accounts with one or more of the IdPs featured in the prototype: Post Office, VISA, Experian, OpenID, GBGroup, or PayPal. The participants were recruited in three age groups, 22 were below 30 (average age 24), 10 were in their thirties (average age 32), and 12 were over-forties (average age 51). .

2.1.2.Prototypes

The prototypes complied with the design principles published by the UK Government's IDA Program. Each screen of the prototypes had only one working link, so there was only one route through the pages. The journeys start at the Service Provider (NHS) home page (see Figure 1).

Next the user goes to a *hub page* where they choose a 3rd party IdP – ideally one they already have an account with (see Figure 2). The user is then directed to the IdP's login page (see Figure 3) where they log in using their normal credentials. On the next screen they give consent for the transfer of their identifying information (see Figure 4) and then arrive back at the NHS pages (see Figure 5), to complete the task they had been set (see next section).

2.1.3.Procedure

Participants viewed only one prototype (Prototype NHS 1 or 2), assigned at random, and were asked to role-play a person who wanted to book an appointment to get their hospital test results, and that this person had an online account with the Post Office. The experimenter sat next to the participant, and asked the participant questions about each page that they saw, including "What would you click on next?". Each prototype page had only one link implemented – to the next page in the user-journey. Participants were directed to the one working link if they chose anything else, and so progressed through all the screens. After the final screen, participants were questioned further about their experiences, and then debriefed. All participants received a £15 Amazon voucher for taking part.

Participants' responses were noted by the experimenter during testing sessions (as close to verbatim as possible). The statements were analysed using Thematic Analysis [2] collaboratively by two researchers: Each statement was read by both researchers, who discussed what theme it represented until consensus was reached. Statements that the researchers could not agree upon or where no clear theme emerged were labelled 'Miscellaneous'. The resulting codes are summarised in Figure 7.

2.2. Results

Figure 6 shows participant continuation and drop-out rates for both NHS1 & 2 prototypes combined, and we interpret it as showing where the pain-points for our participants.. Five participants said they wouldn't continue on the first page of the prototype, because they prefer to transact by phone instead of online. 19/32 the participants viewing the *hub page* said they would stop there, and go to a different channel to complete their transaction. 4/15 of those reaching the page where they consent to or decline the IdP passing validated identifying information about them to the IDA system – said they would not consent and would stop there. Of 44 participants starting the experiment, only 11 said they would continue through the IDA user journey to a page where they returned to the service provider and could carry out their transaction.

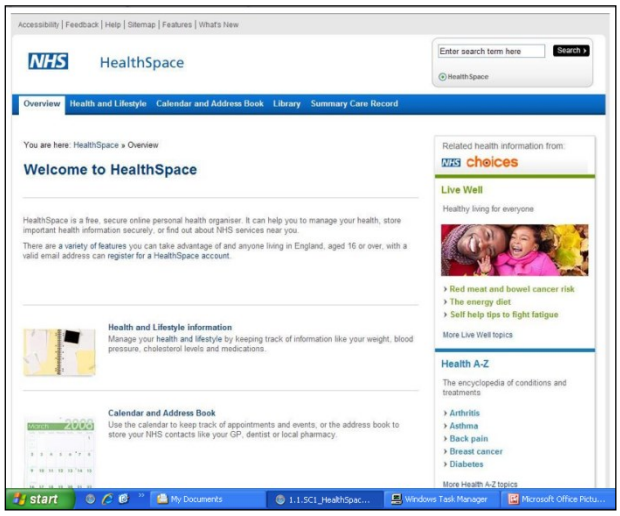

Figure 1: NHS Journey – Relying party 'home page

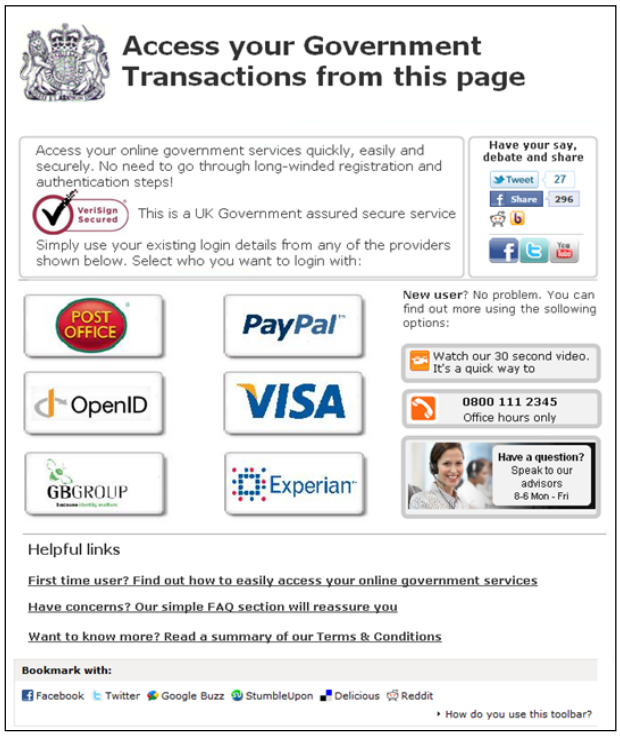

Figure 2: NHS Journey – *hub page* v2

Figure 3: NHS Journey – Identity Provider Login

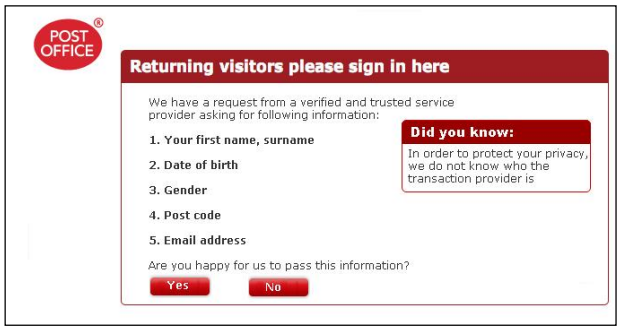

Figure 4: NHS Journey – Identity Provider Consent

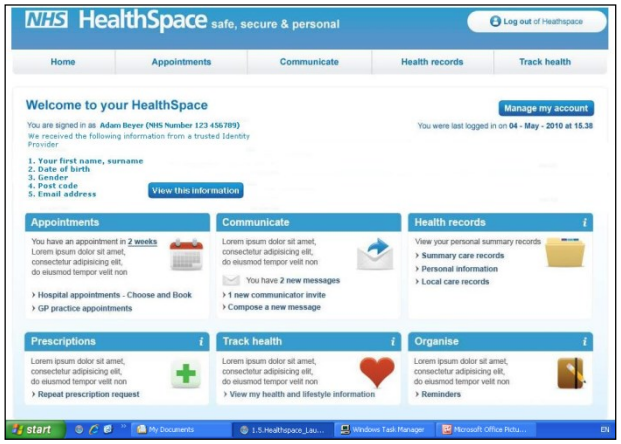

Figure 5: NHS Journey – Relying Party "landing"

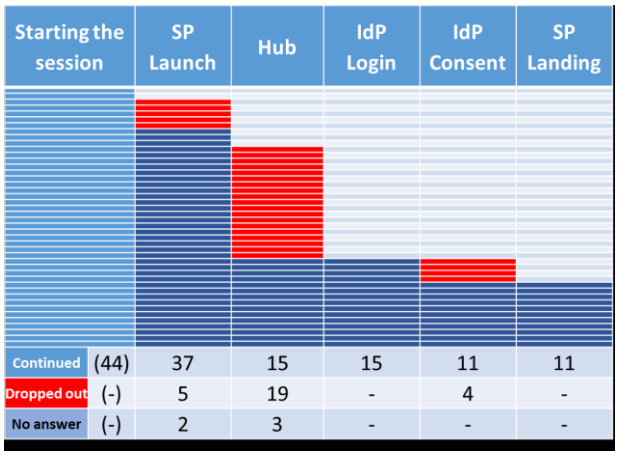

Figure 6: Participant continuation and drop out, for both user journeys NHS1 & NHS2 combined

Our analysis of participants' statements identified some positive perceptions. More than half (56%) of participants *Got the concept* of FedID, saying it was about using credentials from one system on another, and identified some of the benefits this could confer.

"This is simple and will save me time"

"I have an account with one of them so I'll use it"

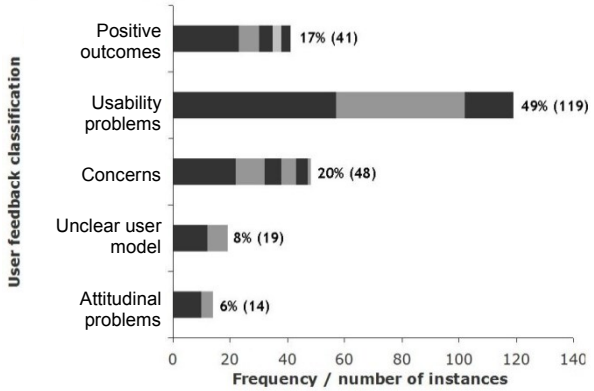

Figure 7: Analysis of participants statements for both user journeys NHS1 & NHS2 combined.

17% of participants *Understood the process*, correctly interpreting what was happening on each screen. 12% *Got the design* , identifying the different parties involved in the process.

49% participant statements revealed usability issues Of these the largest proportion were for improved *Interaction design* (48% of Holistic design issues), improving *Unpredictability of the interaction sequence* and *Lack of coherence* in the user journey, and remedying the problem on the first step of the users' journey - the Service Provider's home page - where there being *No clear call-to-action* meant that people didn't know where to click or what to do to start the journey.

The next largest proportion of usability issues (38%) were lost opportunities for delivering *Reassurance* to users about IDA as a concept and as artefacts they were interacting with. These fell into three types: *Internal (design) reassurance* – page elements that would deliver perceptions that the system was secure and protected the user's personal data – a common example being no lock icons; *External reassurance* delivered to users before their first interaction with the system was also called for (e.g. large publicity campaigns), so that users could come to the system cued to understand it and trust it; and the particular need to *Convey the benefits* of using FedID, that were not apparent to many participants. Example statements:

"Complicated – I'm lost – where is this going?"

"I'd expect logo showing security like padlocks"

20% of participants expressed *Concerns*: Nearly half (46%) of those worried *This is a scam!* – the participants did not believe these were bona-fide government backed projects, but were instead conceived of and implemented by criminals attempting to steal their credentials and commit fraud.. These statements were made by 12/44 participants. 21% expressed *Financial concerns* – a perception that the system would be asking them to pay for services that they usually accessed for free. 13% expressed a *Need for accountability* – that they wanted help or redress if the system caused them difficulty or harm, which was related to their *Privacy* and *Security* concerns (10% and 8% respectively) – would their personal data including login credentials and sensitive records be kept inviolate. 1 participant mentioned a *Lack of transparency* - what would happen to a user's personal data, and the relationships between the counterparties:

"This is a scam – I'd shut it down now!"

"Who is responsible for this is it goes wrong?"

When asked if using the system would enable the Post Office (the IdP in this user journey) to check their medical records at the NHS (the Service Provider) to price their travel insurance, 20% (8/44) said yes.

As Figure 6 shows, the concerns clustered around the *hub page*, and the IdP's *consent page*. Particular issues with the latter appeared to be that participants either did not understand the system's privacy and consent model, and believed that it granted powers to release their data to unknown data processors (leaving themselves with no effective control over their personal data), or they believed that the consent screen was requesting they enter personal data that the website did not already hold, and interpreted this as a phishing attack.

The penultimate class of statements were about *Breaking the user's mental model* (8%), where participants either *Don't get the concept* – not understanding at all what was happening after interacting with the prototype screens, or it *Breaks the mental model* – they do not believe that the transaction parties in IDA have a working relationship: .

"PayPal have nothing to do with the NHS"

The final group of statements revealed valid rejections of the system based on enough understanding of it to have an informed view. These *Attitudinal problems* were comprised of *Compartmentalisation* – that the counterparties in IDA should not have a working relationship, and *Internet refuseniks* – people who believed that some transactions should not be "digital by default":

"Keep government and finance separate"

"I'll only deal with the NHS - directly"

3. STUDY 2: HMRC USER JOURNEY

In Study 2 the high level goal of the user journey was identical to Study 1 – logging in through a third party to access a government service, consenting to the transfer of your identifying information along the way. However the low level details of the scenario differed in terms of the data subject in the transaction, and which Government Service was being accessed through which third party. Participants role-played a small company's Director, and were transacting with information about the business; they had to transact with the UK tax office (Her Majesty's Revenue & Customs - HMRC) about the business' employees, by using a credential belonging to the business. In the scenario, Santander issued this credential to the business for online banking.

Lessons learned from testing the NHS1 & 2 prototypes were used to create a revised user journey in prototypes HMRC1 & 2.

3.1. Method

3.1.1.Participants

Participants were 22 Small to Medium Enterprise (SME) business people, who regularly transact with HMRC through its website, authenticating with the "Government Gateway" (a password based authentication service administered by the UK Government that IDA is intended to replace). Average age was 49 (min. 36, max. 68 years old, s.d. 9.7 years), with 15 male participants and 7 female. Ten (10) were company directors (of businesses with an average of 3 employees), 3 were financial controllers within their business and 9 were accountants or people who do book keeping on behalf of several small businesses.

3.1.2.Prototypes

Two HMRC user journey prototypes were constructed, each having three screens in addition to the NHS prototypes'. Figures 8 to 13 show the screens from the prototype HMRC 2.

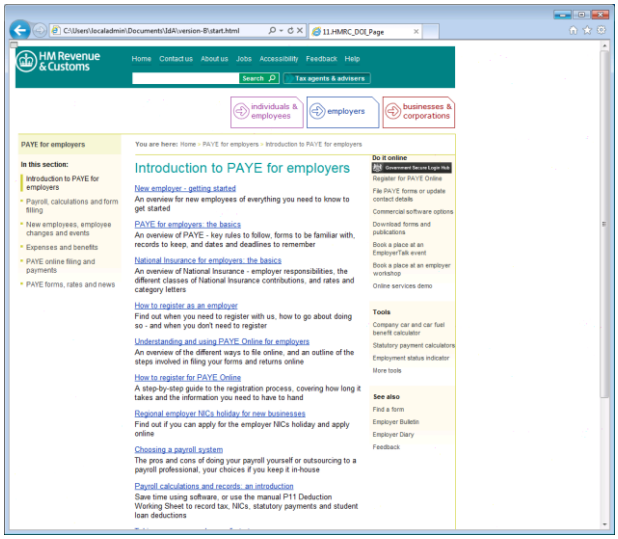

Figure 8: HMRC Journey – relying party *home page*

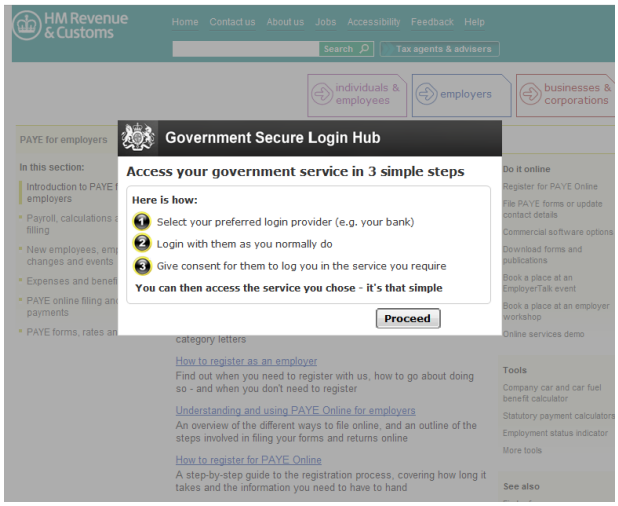

Figure 9: HMRC Journey – *IDA preview page*

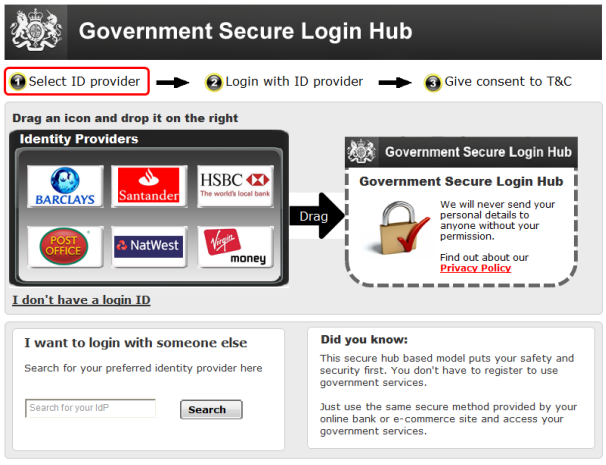

Figure 10: HMRC Journey – *hub page*

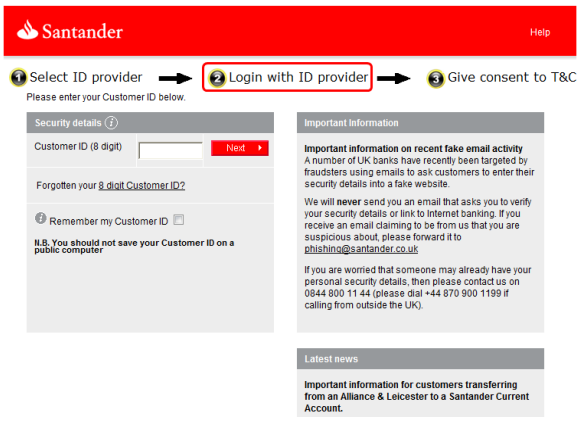

Figure 11: HMRC Journey – IdP *login page*

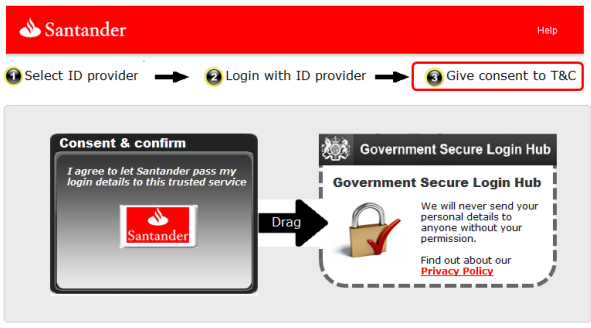

Figure 12: HMRC Journey – IdP *consent page*

Figure 13: HMRC Journey – *hub login status page*

The two HMRC prototypes were identical in function, but differed in some user-interface details. For space reasons we give screenshots for HMRC 2 only, and describe differences between it and HMRC 1.

- HMRC 2's home page (Figure 8) contains an explicit link to the *hub page* that HMRC 1's omitted.
- HMRC2 has a step-by-step overview of the process in its *IDA preview page* (Figure 9), rather than HMRC 1's generic statement about the security of IDA.

- HMRC 2's Hub screen (Figure 10) and IdP's Consent screen (Figure 12) used a drag and drop interaction, whereas HMRC 1 (not displayed) used a click-based interaction style in its equivalent screens.
- HMRC 2 has a progress bar across the top of its windows (in contrast to HMRC1 which omits it – see Figs 10-13)

3.1.3. Procedure

The HMRC prototypes were tested with a procedure that was very similar to the procedure used for testing the NHS prototypes. Participants role-played a user of the system with a particular goal, and answered the experimenter's questions about each page of the prototype. All participants were debriefed and received a £15 Amazon voucher.

3.2. **Results**

Prototypes HMRC1 & 2 showed substantially better retention of users than Prototypes NHS1 & 2 prototypes (Figure 14). Only 19% of HMRC 1 & 2 participants said they would stop by the time they reach the *hub page*, compared to 51% with the previous prototypes – a statistically significant difference (Fisher's exact test, p=0.006). Moreover, only 6% of those reaching the IdP's *consent page* with the new prototypes said they would stop, compared to 27% with the previous prototypes. No statistically significant difference was detected (Fisher's exact test, p=0.172). Power analysis shows that a true effect of this size would require a sample size of 52 per group to have an 80% chance of being detected as statistically significant. Overall, 68% of participants who started the user journey with the new prototypes said that they would continue through to the destination screen, compared to 25% with the previous prototypes, a difference that is statistically significant (Z=3.63, p<0.0001).

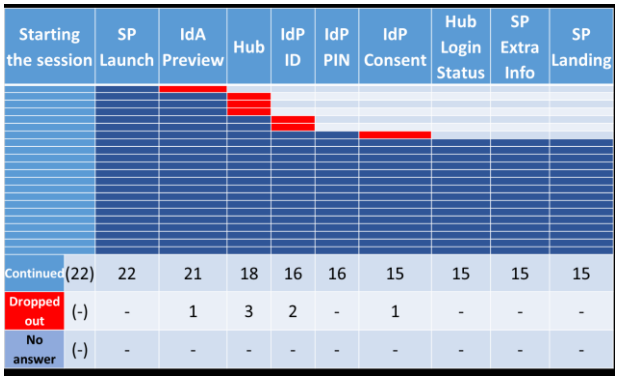

Figure 14: Participant continuation and drop out, for both user journeys HMRC1 & HMRC2 combined

3.3. **Study 3: Online survey**

A central premise of (and FedID in general) is that citizens should be able to (re-) use existing credentials that they hold with existing businesses in order to access Government services. The core of this survey was to assess if the target users willingness to 90 questions that enquired which Government services respondents would or would not access using their use existing credentials / accounts that they hold from for access to e-government services, and if so, which IdPs they would find acceptable, we designed and administered a range of business types survey..

3.3.1. Respondents

104 UK residents were recruited through a UCL psychology department's participant recruitment list.. Average age of respondents was 32.3 (SD = 14.3, min=18, max= 73). 38 declared their gender as female, 21 as male, and 19 did not declare it. In terms of income only 3 respondents declared they were receiving state benefit payments, 66 declared that they were not, and 34 did not answer. 27 respondent declared that their highest qualification was a Higher Degree, 20 that that it was a Degree, and 22 that it was an A-level (e.g. university entrance exam). The majority of respondents (64) held online accounts offering federated identity services that could be used to log into relying parties (e.g. at least one of Facebook, Google, Windows Live, Yahoo, Blogger, Twitter, LinkedIn or WordPress), however, far fewer – only 20 – reported accessing relying party sites with them.

Each respondent could answer one of four questionnaires – see section 2.3.2 for more details. In the first round of recruitment 43 respondents started a questionnaire and 28 completed one. A second recruitment resulted in 60 more respondents beginning a questionnaire, and 47 completing one. In total 75 questionnaires were returned in full, made up of 21 for questionnaire A, 18 for B, 19 for C, and 17 for D.

3.3.2. Survey

Our survey was implemented using the open-source survey engine LimeSurvey 1.91. In order to reduce the time required to complete the survey the 22 business types were split between four questionnaires as follows.

Questionnaire A:
- Your bank for personal banking
- Credit Reference Agency
- The Post Office
- Payment Card Service
- Online Payments
- Your bank for a business account

Questionnaire B:
- Webmail, Calendar, IM, and related accounts (Google, Windows Live, Apple ID, Yahoo!, etc.)
- Online Marketplace (eBay, Gumtree, Loot, Craigslist, etc.)
- Social Network Provider (Facebook, Twitter, Google+)
- Online Retailer (Amazon, Argos, Play.com, etc.)
- Your supermarket (Asda, Lidl, Morrisons, Sainsburys, Tesco, etc.)
- Your insurance company (for Home, Contents, Car, Travel, Life, etc.)

Questionnaire C:
- TV supplier (Sky, Virgin, etc.)
- Telecoms / broadband supplier (BT, Vodaphone, O2, etc.)
- Triple-play supplier – phone, mobile, TV (Virgin, Sky, BT, etc.)
- Your employer
- Online dating site (Match.com, Guardian Soulmates)
- Utility supplier (British Gas, Npower, Thames Water, etc.)

Questionnaire D:
- Travel ticket company (Great Western Trains, thetrainline.com, expedia.co.uk, Easyjet.com)
- A computer account from your old university, or other education institution

- Private healthcare provider
- Transport For London (e.g. Oyster card, bike rental)
- Sports related website (fan site, gym site, club site, etc.)

Every questionnaire covered the same range of Government services:

- Electoral Register
- Passport
- Council tax
- TV Licence
- HM Revenue and Customs, on your own behalf
- HM Revenue and Customs, on behalf of a business
- Benefits
- The NHS
- Driving Licence
- Fishing Rod Licencing.

In order to improve validity and to further reduce the time taken to complete the questionnaires, the questionnaires asked each respondent which of the business and Government services they currently or previously had relationships with, and only displayed questions about those combinations.

We also examined respondents' prioritised requirements for a national FedID system in this survey, with two questions.

The first question was open ended and asked,

> "Please tell us which two or three things you consider to be the most important when accessing Government online services."

The second question was closed response, and asked,

> "Please could you rank the following requirements according to how important you consider them to be in a system you would use to access Government online services with."

The ranked items are shown in Figure 18.

3.3.3. Procedure

Two rounds of recruitment were undertaken, by the Psychology mailing list with a link to a page that redirected respondents to one of the four questionnaires.

The first recruitment redirected respondents at random to one of the four questionnaires. This resulted in an uneven distribution of completed questionnaires between the four versions, so a second recruitment was undertaken.

The second recruitment redirected respondents in sequence to guarantee a more equitable distribution: the first respondent clicking a link was directed to *Questionnaire A*, the second to *Questionnaire B*, and so on with the fifth respondent directed to questionnaire A again, etc.

3.4. **Results**

3.4.1. The market for

3.4.2. FedID access to e-government

The UK Identity Assurance Programme specifies that there should be no privacy implications of using any certified FedID provider to access any e-government services– any combination of IdP and relying parties (RPs) should protect the privacy of the citizen using it : with no RPs (e-government services) should not know who your IdP is, and vice versa. One would expect therefore that all the IdPs should be equally and fully acceptable to citizens. However, they are not: 44% of ratings over all were that respondents *Would Not Use* an IdP to access a Service Provider, with a further 42% being *Undecided*.

Figure 15 shows a summary of participants' willingness to use their business relationships for IDA, summarised by business type.

What is striking is the large variation in the proportion of *Would Use* and *Would Not Use* ratings – our respondents expressed strong preferences and dislikes for different types of IdPs. The *Post Office* was given the largest proportion of *Would Use* ratings – 70%- whereas utility companies were given 4% - the least.

Respondents were more positive towards they idea of 'everyday businesses' (such as webmail providers, supermarkets, banks, online retailers) as IdPs than we had expected. They were also positive towards their employers acting as their IdPs. Businesses that received negative ratings were Online Social Networks (OSN) – Credit Reference Agencies (CRAs), Internet Service Providers (ISP) and phone companies, and utilities.

The significant difference between businesses that offer communication services was surprising: Webmail, Calendar, IM, and related accounts (Google, Windows Live, Apple ID, Yahoo!, etc.) received more 'would use as IdP' votes than OSNs (Facebook, Twitter, Google+)" ($Z = -3.43$, $p = 0.001$). Comments indicate that that respondents seemed to be wary of the broadcasting nature of OSNs:

> "Worried that my hospital details would be broadcast on Facebook if I pressed the wrong button".

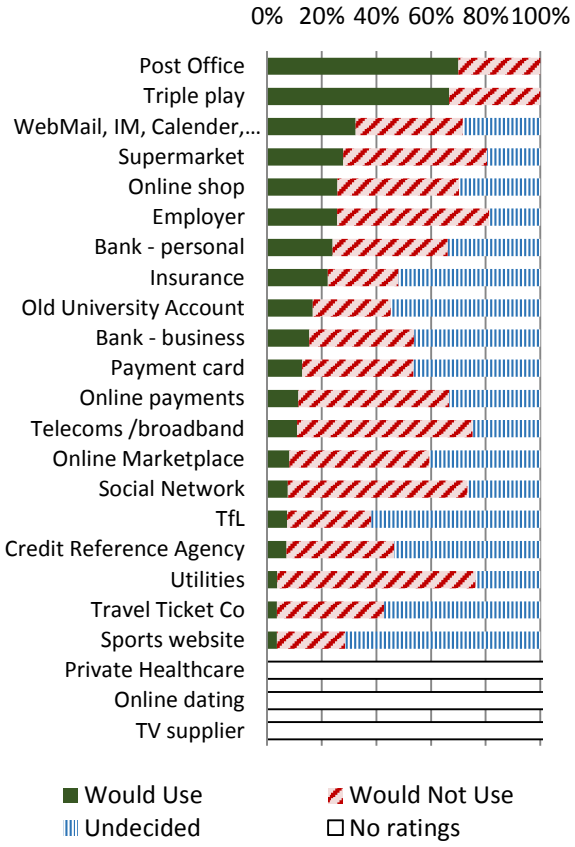

Figure 15: Respondents' self-predicted use of Identity Providers for IDA

There are some positive outcomes for IDA from this data. While there are an average of 44% of *Would Not Use* bars, *Would Use* bars are present too – our sample's average was 14% of ratings being affirmative (see the leftmost bars in Figures 15 & 16). These respondents said that they would use their relationships with a wide range of business types in order to access e-government services. This supports the mission of the UK IDA programme, since some citizens would immediately be willing to use some of their existing online credentials to access e-government. If these results are representative of the national picture, a large number of those UK citizens who are educated and used to transacting online would make the transition easily. However, this may only be a small proportion of citizens overall.

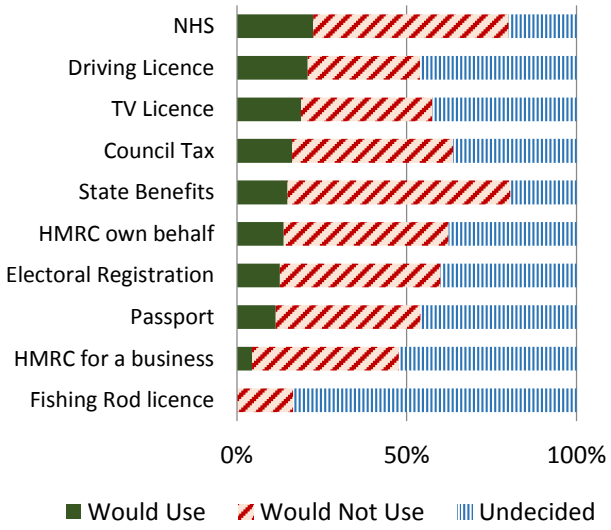

Figure 16: Respondents' self-predicted use of IDA with Relying Parties

Figure 16 shows a summary for each Government Service we studied across all business types. There were many negative responses: an average of 44% said they would not use their existing online credentials to authenticate to access e-government services. Taking Figures 15 and 16 together, we see that respondents have preferences about which IdPs they would use and - crucially *would not use* - to access Government services, and which Government services they would access through IDA. More accurate determination of what these preferences are, and in what proportions will require follow up work.

This result may be seen as consistent with Roger's technology adoption lifecycle [cf. 17], and a normal response to new technologies being applied in established transaction contexts. Roger's technology adoption lifecycle describes the diffusion of new technologies through populations, where adoption follows the same pattern irrespective of the technology (although adoption may stall, depending on aspects of the technology such as its usability). In this model new technology is first taken up by a small number of risk-oriented and wealthy "innovators" before spreading through other larger, more risk-averse and less financially secure segments of the population.

Our data tends to support this – Figures 15 and 16 also display many *Undecided* bars: respondents who did not actively feel they would or would not use businesses as IdPs – with an average of 42% of all ratings. For half of the Government Services we asked about, more participants said they were undecided about using businesses as IdPs, than said they would NOT use them for this purpose. So currently, it the largest group of citizens are neither for nor against FedID solutions for e-government – their attitude is 'wait and see'.

3.4.3. Citizens requirements of an IDA system

Our survey also attempted to elicit citizen requirements for an e-government IDA system, and in two ways – by giving them a free response question (Figure 17), and giving them a list of hypothesised benefits to rank (Figure 18).

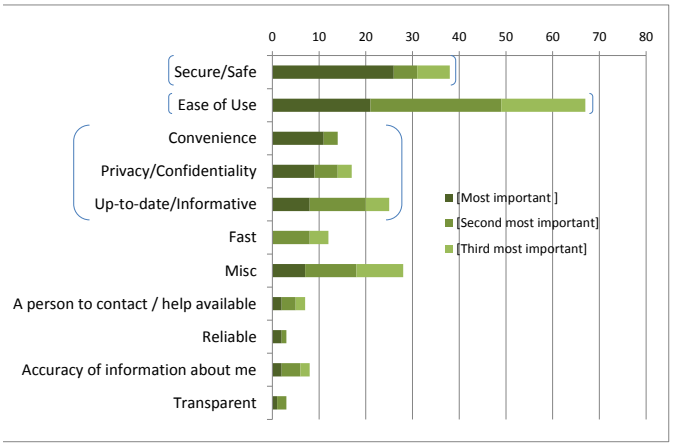

Figure 17: Three most important requirements for IDA systems; open question responses. Requirements in different brackets had statistically significantly different proportions of respondents ranking them as most important, at p > .05

Figure 17 shows the benefits that respondents volunteered as those they would wish for from an Identity Assurance system, collected into themes. The chart shows a count of how many times items of each theme were stated as being most important, 2nd or 3rd most important, etc., and is sorted by frequency of being mentioned as most important.

Secure / Safe was the requirement most frequently expressed by respondents as most important, using phrases such as,

- Security (19 people)
- Safe and Secure (2 people) and Safety (2 more)

However, it was not statistically significantly more often cited as the most important than the next most frequently cited theme - *Ease of use* ($Z=0.77$, $p = 0.44$). The proportion of times *Ease of Use* was listed as second most important greatly exceeds that of any other theme, and boosts its overall proportion of mentions to significantly more than any other theme's, including *Secure / Safe* ($Z = -3.17$, $p = 0.002$). This highlight's the critical importance of usability in any national e-ID scheme.

Phrases used for requirements of this type included,

- User friendly (6 respondents)
- Ease of use (10 respondents)
- Ease of navigation (7 respondents)
- Clarity of information (7 respondents)

The next group of requirements were significantly less frequently mentioned as most important than *Ease of use* ($Z=-1.97$, $p=0.048$), but at an equivalent level to each other. These included *Convenience*, with items such as:

- Ease of access (5 respondents)
- Easy access (4 respondents)

Also *Privacy/ Confidentiality*, with items such as:

- Privacy (6 respondents)
- Confidentiality (6 respondents)

Up-to-date / Informative / Helpful, relates to the quality of services available by using the FedID, with items such as:

- Has information relevant to me (4 respondents)
- Up-to-date information (3 respondents)
- Regularly updated content (1 respondent)

Up-to-date/Informative is significantly more highly rated than the next most highly rated theme – *Fast* (Z=-2.39, p=0.017), which in turn is statistically not significantly different to the themes that follow it.

Of the IDA benefits suggested to respondents (see Figure 18), the most highly ranked benefit was *Increased security*. The next most highly ranked was *Saves you time*. These are not statistically significantly different to each other (Z = 1.71 p = 0.086). *Increased Security* was however statistically significantly more popular than *Reduced bureaucracy* (Z = 3.59 p< 0.0001) – the third most highly ranked possible benefit.

Saves you time is almost statistically significantly more valued than *Reduced bureaucracy* (Z = 1.85 p= 0.064), and definitely is more popular than all the lesser valued benefits (Z = 2.09 p= 0.036). *Reduced bureaucracy* and *Reduced costs to taxpayers* are as highly valued as each other, and statistically significantly more valued than the remaining benefits.

While a few respondents (less than 10%) valued *Increased opportunities for UK businesses* the most of the possible benefits, nearly 40% valued this less than all other benefits. Similarly *Fewer passwords to remember*, *You will remember your login details more* and *Avoiding signing up for new credentials* were not as important to respondents as other benefits.

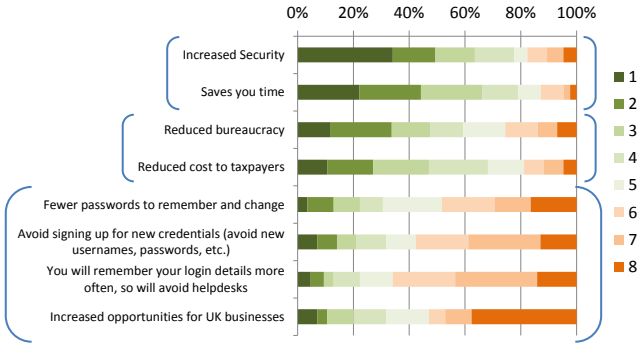

Figure 18: Respondents' rankings of Government generated IDA system requirements, from 1 (most important) to 8 (least important). Requirements in different brackets had statistically significantly different proportions of respondents ranking them as most important, at p > .05

4. DISCUSSION

In our survey, both ways of measuring what respondents value in FedId for access to e-government services (e.g. the ranking exercise and the open question) bring out the importance of security and safety. It was the theme most frequently mentioned as being most important. *Privacy and confidentiality* are something that respondents value – approximately as much as *Convenience* – that the system should be 'easy to access'. *Ease of Use* as a concept also ranks highly in the open question section. In this sample at least, the number of times it was mentioned as *most important* is not significantly different to *Secure/Safe*, but it is more frequently mentioned overall, and is the most frequently mentioned theme. *Reduced bureaucracy* and *Reduced cost to taxpayers* were not mentioned unprompted - but when suggested to them in the ranking exercise they were ranked important relative to other requirements. This suggests that there is scope for improving citizen awareness of these benefits when marketing FedID and e-government. *Speed* and the related *time saving* are important in both open questions and the ranking exercise. *Transparency* does appear in responses to the open question , but ranks low overall.

As in previous research with UK citizens [4], our respondents wanted assurance that transition to online does not equal *'you're on your own'* that there should be easy to get human assistance when needed, and redress and restitution if something went wrong..

Webmail providers (such as Google and Yahoo) were relatively popular as possible IdPs – especially younger respondents said they would use them to access e-government services. This concurs with work that found increasing privacy concerns about internet with age, with nearly double the respondents aged 40+ having concerns compared to those aged 20 or less [12]. In contrast, OSNs (such as FaceBook and Google+) were relatively unpopular as IdPs – far more people were not willing to access Government service through them. This is a key finding in view of the success of – FaceBook Connect – the 600 pound Gorilla in the space FedID. It suggests that people are aware of the privacy implications (and the UK government has ruled out FaceBook as an IdP, on those grounds) but the comments also show that – similar to Riegelsberger's results in the early days of e-commerce [14] they do not feel entirely competent in this new space, and fear that they might broadcast confidential information by mistake.

Online payments businesses (e.g. PayPal) were also relatively unpopular as IdPs - very few respondents were willing to access e-government services through them, and more than half said no. Credit Reference Agencies were also not popular, Whilst our sample size was small, it suggests that work that awareness of the benefits of using financial sector providers as IdPs needs boosting...

4.1. CONCLUSIONS

4.1.1.Improving acceptability of FedID for e-government

Our studies asked participants to look at prototype user journeys. On each screen they were asked would they continue or stop. Drop-out rates in the first prototype study were – especially given the level technology-literacy of our participants – alarming. The fact that changes to the prototype for the second study led to a lower drop-out rate shows that usability design needs to be part of the rescue plan, but there was still a significant drop-out rate that shows there needs to be more preparatory communication – FAQs and hands-on demos with people on hand to answer citizens' questions..

4.1.2.Improve communication about privacy features

To protect citizens' privacy, the UK FedID system specification prevents RPs and IdPs from communicating directly, and even knowing who their transaction parties are. Our findings show that the benefit of this approach is not obvious – and even worse, our participants inferred the system was NOT secure –

which is their top requirement. Current mental models of trust rely on knowing the transaction partner [15], and this means that to the citizen at least, the recipient of their citizens personal data must be identified. That, of course, would undermine the privacy protection the system was designed to offer. This is a fundamental conundrum that needs to be addressed, urgently.

4.1.3. Citizens requirements for National FedID

There appear to be three core benefits that respondents desire from National Federated e-ID systems.

(a) Respondents rated *Security* as the most important benefit.
(b) *Ease of use* and *saves you time* are key properties that respondents also valued.
(c) *Reduced cost to taxpayers* and *Reduced bureaucracy* were also highly valued.

4.1.4. Some IdPs more acceptable than others

Some transactions between citizens and Government will require more rigorous protection than others, and this has been codified into *4 levels of assurance,* with higher levels requiring more elaborate, effortful and certain proofs of identity. The IdA system design presented to participants in our prototypes made no reference to these levels of assurance; all IdPs presented to participants were not differentiated according to the types of transactions they were able to protect. Moreover, neither did we mention levels of assurance when we questioned participants about which possible IdPs they might use for which Government services. We had assumed that all IdPs would be able to offer services that protected citizens' privacy equally whatever their transactions with whichever relying party. However, respondents still appeared to have preferences over which kind of business they would be willing to use to gain access to e-government services.

We asked survey respondents which of a range of business types they would be willing or not willing to use as their Identity Provider (IdP) to access a range of government services in a Federated National e-ID system. In general, more respondents were definitely *not willing* to use each kind of business as an IdP than were definitely willing to use it – in a ratio of about 3:1.

However, for about half the government services we asked about, more respondents had no strong feelings about using their relationships with businesses for IdA than said they definitely did *not* want to use these relationships for IdA. About twice as many said they had no strong feelings than said they definitely *would* use their existing accounts for IdA.

Extrapolating from this data, it is plausible that many citizens could to persuaded to use FedID for transactions with e-government, provided their requirement – with security, ease of access and . Each Government service in the survey had at least one business type that some participants would be willing to use as an IdP to access it with, so the IDAP focus of delivering IdP choice for the citizen is supported by this data.

4.1.5. More than a 'user interface' problem

Our studies show that conventional usability techniques can do much to improve the understanding and acceptability of FedID for e-government transactions,. However, there are things to be done beyond the interface: participants were distrustful of a system that disrupted their expectations by establishing relationships between organisations that they believed did not and should not be involved in their relationship with government, and that - while *risks* of such a system were apparent to them - the *benefits* were not. Citizens need to be better - but honestly - informed about the risks and benefits of authenticating to government in this way, and government needs to provide accessible support in case of problems, and effective redress and restitution if anything goes wrong.

4.2. Further research

The participants in our second prototype testing study had all experienced the UK's Government Gateway – an authentication system that has received criticism for the burdens placed upon it's users, and that IDA is meant to replace. This experience could have given our revised prototypes a greater perception of usability and acceptability, compared to how they might be perceived by users without that experience. We did not know if participants in our first prototype study had used the Government Gateway or not. We therefor recommend that further work should sample participants from populations that come to transact with the Government online for the first time, as well as populations that have used the Government Gateway, to see how it influences people's reactions to IDA.

The Identity Provider's Consent screen was redesigned from the first prototype study to the second study, naming the known intermediate recipient of the users' identifying data (rather than saying only that the final recipient was unknown) and introducing a direct manipulation interaction style where the user dragged their personal data and dropped it onto the named recipient. This redesigned Consent screen was an improvement. Conventional user interfaces for giving consent include tick boxes or OK buttons, and are very accessible to people who have disabilities of various kinds. They suffer from the disadvantage of being easily dismissed by users who instinctively act upon perceiving an alert without taking in what they are consenting to. Direct manipulation interfaces in contrast do have accessibility problems, for example where visually impaired users may not be able to see the icons to drag and drop them. However, they may require users to pay more attention to the consent choice they are making, by forcing users to manipulate their personal data directly and attend to the destination they are sending it to. Further work should therefore explore if positively identifying the recipient of users' identifying data (even if the recipient is an intermediary and not the final recipient) using conventional mechanisms such as tick boxes is enough in a consent screen, or if direct manipulation interfaces confer substantial advantages by increasing user attention and comprehension.

Finally, the data we present on citizens preferences for IDA system benefits and which businesses they would use or not use as IdPs is based on a small and nationally unrepresentative sample. We recommend that these issues be explored with far larger surveys with representative samples of respondents, and enough respondents to give good precision.

5. REFERENCES

[1] Bracken, M. (2012). *Identity and Privacy Principles*. http://digital.cabinetoffice.gov.uk/2012/04/24/identityand-privacy-principles/

[2] Braun V. & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), pp.77–101.

[3] Cameron, K. 2005. *The Laws of Identity.* Retrieved April 1, 2013, from Kim Cameron's Identity Weblog: http://www.identityblog.com/?p=352

[4] Crane, S., Lacohee, H., & Zaba, S. (2006). Trustguide -- trust in ICT. BT Technology Journal, 24(4), 69-80.

[5] Dhamija, R., & Dusseault, L. (2008, March/April). The Seven Flaws of Identity Management: Usability and Security Challenges. *IEEE Security and Privacy*, 6(2), 24-29

[6] Florencio, D., & Herley, C. (2007). A large scale study of web password habits. Paper presented at the WWW 2007, Banf, CA.

[7] Fowler, G. A. (2012, 4th October). Facebook: One Billion and Counting, The Wall Street Journal. Retrieved from http://online.wsj.com/article/SB10000872396390443635404578036164027386112.html

[8] Friedman, B., Millett, L., Felten, E. (2000). Informed consent online: A conceptual model and design principles. UW CSE Technical Report 00-12-02. Seattle, WA: University of Washington, Department of Computer Science and Engineering.

[9] Inglesant, P., & Sasse, M. A. (2010). *The true cost of unusable password policies: password use in the wild.* Paper presented at the CHI 2010, Atlanta, GA.

[10] Jøsang, A., AlZomai, M., and Suriadi, S. (2007). Usability and Privacy in Identity Management Architectures. *Proceedings of the Australasian Information Security Workshop (AISW'07)*, Ballarat, January 2007.

[11] Krol, K., Moroz, M. and Sasse, M. A. (2012). Don't Work. Can't Work? Why It's Time to Rethink Security Warnings. Paper presented at the *7th International Conference on Risks and Security of Internet and Systems (CRiSIS 2012)*, 10-12 October 2012, Cork, Ireland.

[12] Paine, C., Reips, U.-D., Stieger, S., Joinson, A. and Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies,* 65, 526-536.

[13] Rahaman, A, Sasse, M. A. (2010) A framework for the lived experience of identity. *Identity in the Information Society*. 3(3), 605-638. Available at: http://dx.doi.org/10.1007/s12394-010-0078-3

[14] Riegelsberger, J., & Sasse, M. A. (2000). "Trust me, I'm a. com" The problem of reassuring e-shoppers. *INTERMEDIA-LONDON-, 28*(4), 23-27.

[15] Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies, 62*(3), 381-422.

[16] Rogers, E. M. (1982) *Diffusion of Innovations*. Free Press, New York.