Conceptualising the Lived Experience of Digital Identities towards Federated eGovernment Identity Management

Susan Zhuang

Project report submitted in part fulfilment of the requirements for the degree of *Master of Science (Human-Computer Interaction with Ergonomics)* in the Faculty of Brain Sciences, University College London, 2012.

NOTE BY THE UNIVERSITY

This project report is submitted as an examination paper. No responsibility can be held by London University for the accuracy or completeness of the material therein.

ACKNOWLEDGEMENTS

I would like to thank Angela Sasse for supervising my project; as well as Charlene Jennett and Sacha Brostoff for their guidance and advice in the completion of my project. I am also grateful to all the participants who contributed with their time and interest in this study. This dissertation would not have been possible without them.

My thanks go to my personal tutor, Duncan Brumby, and all UCLIC staff and coursemates, in particular Team Feelybean, for their invaluable support and encouragement throughout this MSc course. It has been a joy and an honour to work and share great moments with you all over the past year.

Last but not least, I would like to thank my dear Michael for proofreading my thesis drafts, and for showing unending support, motivation, and interest throughout my studies.

ABSTRACT

Literature identifies numerous usability problems associated with managing multiple online accounts, such as users' propensity to use the same password across accounts. Federated identity management systems (FIDMS), allowing a single login to access several accounts, are fast becoming an attractive solution to these problems. In particular, FIDMS for eGovernment services may facilitate seamless and integrated experiences of government activities, and reduce administration costs for government departments. This necessitates re-examination of 'digital identity' and multiple user account management for implementation in an eGovernment context. Digital identity research is predominantly technology-centred, focusing on technological feasibility and organisational utility, rather than the underlying human factors of identity management. This study aimed to develop a *user-centred* understanding of digital identity for eGovernment, managing multiple eGovernment accounts in everyday life, and perceptions of eGovernment FIDMS. An exploratory, qualitative approach was taken, using semi-structured interviews, and video diary studies capturing 15 users' *in situ* interactions with eGovernment user accounts over two weeks. It was found that users conceptualise eGovernment digital identity as a disembodied, multifaceted, and context-dependent construct. Digital identity was found to belong in a layered identity ecosystem, relating to the individual, technology, organisation, society, and ethics. Everyday life interactions with eGovernment were found to be compartmentalised and task-driven, influenced by the dynamic nature of users' needs and life situations, and the interplay between task, physical location, and device. Problems with managing multiple accounts were observed, pointing towards benefits of FIDMS. However, users had reservations pertaining to security, privacy, and information relevance. Design implications for user-centred eGovernment FIDMS were developed, such as accounting for continuous changes in user needs, and facilitating completion of primary task while reducing the interruptibility of login procedures.

TABLE OF CONTENTS

CHAPTER 1 **INTRODUCTION** **9**

CHAPTER 2 **LITERATURE REVIEW** **12**

2.1. Identity & Digital Identity **12**

2.1.1.What is Identity? 12

2.1.2. Conceptualising Digital Identity 14

2.2. Federated Identity Management **16**

2.2.1. Multiple Partial Identities 16

2.2.2. Identity Management 18

2.2.3. Federated Identity Management Systems 20

2.3. Identity in eGovernment **22**

2.4. The Lived Experience of Identity **26**

2.5. Research Questions **27**

CHAPTER 3 **METHODOLOGY** **29**

3.1. Design **29**

3.1.1. Semi-Structured Interviews 30

3.1.2. Video Diary Study 31

3.1.3. Grounded Theory 33

3.2. Participants **34**

3.2.1. Recruitment Questionnaire 35

3.2.2. Selecting Online Accounts 37

3.3. Procedure **39**

CHAPTER 4 **RESULTS** **41**

4.1. Levels of Interaction **43**

4.1.1. Individual 43

4.1.2. Technological 44

4.1.3. Organisational 47

4.1.4. Societal 48

4.1.5. Ethical 50

4.2. Contexts of Interaction **51**

4.2.1. Task & Purpose – What users do and how they do it 51

4.2.2. Location & Device – Physical contexts 53

4.2.3. Time & Life Situation – The effects of time and dynamics of life 55

4.3. Perceptions of FIDMS **57**

4.3.1. Multiple Separated Accounts 57

4.3.2. Federated Accounts **58**

CHAPTER 5 **DISCUSSION** **61**

5.1. The Lived Experience of Identity **61**

5.1.1. A User-Centred Perspective of Digital Identity 61

5.1.2. Levels of Interaction: The Identity Ecosystem 64

5.1.3. eGovernment Identity in Everyday Life 67

5.2. Design Implications for eGovernment FIDMS **69**

5.3. Limitations **71**

5.4. Future Work **73**

CHAPTER 6 **CONCLUSION** **75**

REFERENCES **77**

APPENDICES **86**

Appendix A. Recruitment Questionnaire 86

Appendix B. Informed Consent Form 90

Appendix C. Information Sheet 91

Appendix D. Briefing Script 92

Appendix E. Interview Questions 94

Appendix F. Video Diary Instructions 97

Appendix G. Examples of Transcripts 100

CHAPTER 1 **INTRODUCTION**

The UK government is increasingly digitising its public sector services towards eGovernment, i.e. online relationships between governments, citizens, and organisations (Jeong, 2007). Digital implementation of services such as the National Health Service (NHS) and HM Revenue & Customs (HMRC) provide users with the opportunity to create user accounts to store and retrieve their personal information; and interact with the service. This has numerous advantages for people, including convenience and empowerment in daily life activities (Mäkinen, 2006); as well as for government, in saving administration costs (McKenzie, Crompton, & Wallis, 2008).

With an increasing number of government organisations offering their services online, people find themselves managing an increasing number of user accounts, each distributing their personal information to different channels (Lips & Pang, 2008). Improving identity management systems, i.e. systems for representing and recognising entities (individuals and organisations) in computer networks (Jøsang & Pope, 2005), is needed to address this digital bricolage of identities.

Federated identity management systems (FIDMS) are proposed as a viable solution to the problems of managing multiple user accounts. A FIDMS is '*a set of agreements, standards, and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a federated domain'* (Jøsang & Pope, 2005). This implies that users need only apply their login details once, and subsequently have access to their accounts with other service providers (SPs) within the same federation. There are disadvantages to this, most significantly the increased security risk of having numerous pieces of personal information correlated under a single access point (Camp, 2004b). However, users are found to adopt counterproductive and security-compromising strategies to cope with their multiple online accounts, such as using the same password across accounts (Adams & Sasse, 1999). FIDMS has substantial potential to integrate activities to create the seamless experience of a *'joined-up government'* (Pollitt, 2003).

In order to best develop FIDMS for eGovernment, a significant research gap must be addressed, namely the lack of a user-centred perspective of: i) digital identity; ii) multiple user accounts in everyday life; iii) and eGovernment interactions (Cameron, 2005; Jøsang & Pope, 2005; Dhamija & Dusseault, 2008; Rahaman, 2012). Identity research thus far has been technology-centred, i.e. looked into issues such as organisational cost-effectiveness, security and privacy concerns, and technology-specific usability problems. Hence, there is a lack of understanding of the *'lived experience'* of identity (Rahaman & Sasse, 2011), i.e. the human factors that underlie interactions with digital representations of individuals' personal information and their relationships to the authenticating organisation. Indeed, digital identity is arguably not only a technological concern, but an organisational and societal concern as well (Cranor & Reagle, 1998). Several issues need to be explored and refined in order to achieve user-centred FIDMS, such as: how do users relate to the digital representation and distribution of their personal information? What is the reality of user interaction with eGovernment accounts in everyday life? What are users' perceptions of federated identity systems?

To address these questions, an exploratory, qualitative study was conducted. Semi-structured interviews with users of eGovernment services were conducted to gauge users' perceptions of and attitudes towards their digital identity, disclosure of personal information online, management of multiple user accounts, and government services. In order to verify and extend these insights, a two-week video diary study was conducted to collect observational data on users' actual behaviour when interacting with user accounts for government services *in situ*. It was found that users perceive digital identity as disembodied facets of identifying information, contextually bound to the purpose with each service. Moreover, users interact with their digital identity not only on a technological, interface-specific level, but also on individual, organisational, societal and ethical levels. Further to this, external and dynamic influences of everyday life, such as changing employment and physical locations, affect the interaction with eGovernment accounts.

This dissertation is outlined as follows: Chapter 2 presents a review of existing literature, identifies the research gap, and establishes the research questions; Chapter 3 describes the research methods used in the present study to address the research questions; Chapter 4 presents the main outcomes of the data analysis; Chapter 5 discusses the outcomes in the context of reviewed literature, proposes design implications, and outlines the study limitations and suggestions for future work; and Chapter 6 summarises the research project, evaluates its merits, and concludes with its contributions to digital identity and eGovernment FIDMS research.

CHAPTER 2 **LITERATURE REVIEW**

The following literature review provides the background for discussion of the relevance and importance of digital identity and user-centred FIDMS for eGovernment services. A research gap is identified wherein the limited understanding of users' lived experience of interacting with multiple accounts in daily life is highlighted. Finally, research aims and questions for the present investigation are stated.

2.1. Identity & Digital Identity

The identity construct and its purpose in society is important to establish in order to understand the role of digital identity in individuals' daily life, and its implications for eGovernment interactions. This section describes definitions and purposes of identity, highlighting the multifaceted nature of identity, and important properties of digital identity.

2.1.1.What is Identity?

Existing literature is lacking in a unified and user-centred definition of 'identity'. In society, identity is traditionally a means of making an individual identifiable; such that one can receive the services and benefits one is entitled to, as well as prevent the actions one is restricted from performing (Cottrell, 2010; Rahman, 2012). Identity can be used for a wide range of purposes, including accessing restricted areas such as buildings or bank accounts, and to understand social orders within a community (Williams, Fleming, Lundqvist, & Parslow, 2010; Rahaman, 2012). As identity helps define an individual's social role, the characteristics and attributes that make that individual recognisable to the agent authenticating[1] the individual are crucial (The Cambridge Dictionary of Philosophy, 1995; Chadwick, 2008). Such attributes or '*assertions of truth*' (Cameron, 2005) may both be '*a set of permanent or long-lived temporal attributes associated with an entity*' (Camp, 2007), such as name or blood type; and '*a set of characteristics, or* ***identifiers****, of an entity that uniquely identifies that entity within a specific context or system*' (White, 2008), such as occupational role or Unique Tax Reference number. These definitions strongly suggest that identity cannot be described in straightforward terms as a single, unified construct (Buckingham, 2008).

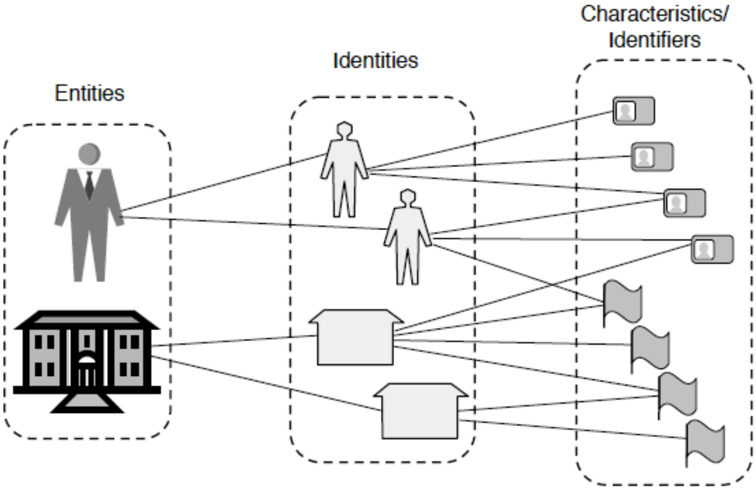

Figure 1. An identifiable entity can either be an individual or an organisation. Each entity can have multiple identities, depending on the context of use. Each identity can have multiple identifiers (card symbol = user identifier; flag symbol = SP identifier) (Reproduced from Jøsang & Pope, 2005).

Rather than having '*an* identity', individuals arguably have multiple identities (Figure 1), each with their own purposes and constraints. (Alpár, Hoepman, & Siljee, 2011). Durand (2003) described 3 tiers of identity: the personal identity, controlled by the

[1] Authentication: the process whereby the presented identifying information is validated (Rahaman, 2012).

individual and therefore subjectively conceived to be their true, inner identity; the assigned identity, temporarily issued to the individual by other agents to be used in a particular context, for example employment titles or phone numbers; and the ‘abstracted or aggregated’ identity, i.e. the identity resultant from aggregating an individual’s properties, e.g. ‘young Caucasian male, student, and interested in skydiving.’ Consequently, identity is not necessarily absolute, as it may change over time (Alpár et al., 2011). Nor is identity necessarily unique, as individuals may be identified as belonging to a larger group with similar aggregated attributes (Jøsang & Pope, 2005; Alpár et al., 2011).

2.1.2. Conceptualising Digital Identity

The move from paper-based forms of identity, such as passport documents and birth certificates, to digital forms of identity necessitates an even more encompassing view of identity. The identifiers of ‘digital identity’ concern a digital entity or its connections to other digital and/or non-digital identities (Windley, 2005). Such identifiers may include digital representations of pre-existing personal information, e.g. name, date of birth, and blood type; but also extend to digitally *assigned* identity information (Jøsang & Pope, 2005), e.g. email addresses, IP addresses, usernames and passwords (Greenwood, 2007). Given their external assignment, such identifiers are normally meaningful only in specific contexts (Camp, 2004a).

A key element of digital identity is the absence of face-to-face interactions when utilising services, causing a disembodiment of identification processes (Rahaman, 2012). It is important to address the implications of the resultant differences between digital and physical identity. The lack of confinement to physical location and limited networks (Camp, 2003) entails a wider, and potentially freer, distribution of personal information across more numerous and remote locations (Norlin & Durand, 2002), as interaction transcends space and time (Taylor, Lips, & Organ, 2006). Digitised personal information may introduce remotely located parties – identified individuals and identifying organisations – to each other significantly more effectively and efficiently than in the physical realm (Damiani, de Vimercati, & Samarati, 2003). Moreover, the reduction of physical and temporal boundaries between individuals and organisations implies that organisations' capabilities of relating to and performing surveillance of individuals no longer relies on physical presence (Taylor et al., 2006), but instead on individuals' digital transactional history (Camp, 2004b). This is of significant consequence in today's globalised society.

Simultaneously, the disembodied nature of digital identity has numerous advantages for the user as well. The digital realm allows for withholding of identifiable information, anonymity, and pseudonymity (Camp, 2004b; Lips & Pang, 2008). Hence, the concealment of personal information made possible by the physical distance between individuals and organisations may increase the level of privacy and limit individuals' public availability (Clarke, 1997; Crompton, 2002; Gilbert, Kerr, & McGill, 2006). This may ensure boundaries are kept between the user and the organisation (Pfitzmann et al., 2006).

The dynamic properties of digital identity are also important to address. Unlike invariant identifiers typical of physical identities, such as date of birth and fingerprints (Maler & Reed, 2008), digital identifiers, such as usernames and IP addresses, can dynamically change by being deleted and replaced with new identifiers (Jøsang & Pope, 2005). Lacking in human-computer interaction (HCI) literature are users' perspectives and experiences of digital identity, i.e. how they relate to its dynamic and disembodied properties, and how they experience identifying themselves digitally.

2.2. Federated Identity Management

To ensure that users accept an identity management system (IDMS), optimal user-centred design is essential. Thus, it is important to understand the usability problems of managing multiple user accounts online. This section decomposes digital identity as multiple partial identities, and discusses the associated usability problems. Federated identity is described and proposed as a solution to these problems, before the next section places FIDMS in the context of eGovernment.

2.2.1. Multiple Partial Identities

Digital identity does not exist in a vacuum, as identifying information about the user is distributed to several different online sources via multiple user accounts. As in the real world, where an individual may have one relationship with the NHS where they exchange personal health information, and another relationship with the HMRC where they exchange tax information, digital identities are also dependent on the online domains in which they are applied (Rahaman, 2012). A digital identity therefore represents a 'partial identity', i.e. the context-dependent subset of the aggregated personal information attributes of an individual (Damiani et al., 2003; Pfitzmann & Hansen, 2010). To illustrate, a partial identity in the context of shopping has e.g. credit card details as identifiers, while the identifiers for a partial identity in healthcare are e.g. allergies and prescriptions (Pfitzmann & Hansen, 2010).

Multiple partial identities are regulated by contextual boundaries. Goffman (1959) argues that individuals selectively disclose personal information to adapt to varying circumstances. Hence, depending on factors such as the individual's purpose with interacting with another party, the identity individuals present vary widely (Goffman, 1959). Extending this, Altman (1975) described a framework of dynamic boundary regulation: the protection and disclosure of personal information is a continuous process of optimisation as the individual's goals, and therefore boundaries, change according to context. In digital environments, such boundaries are represented in the multiple user accounts an individual has: access to specific properties of the user's identity is selectively granted to specific parties (Lips & Pang, 2008). There is limited understanding of how users perceive these boundaries, particularly regarding what personal information they are more and less willing to disclose.

It is firmly established in HCI literature that managing these accounts face numerous usability problems. The resultant '*patchwork of identity one-offs'* due to managing separate relationships with SPs (Cameron, 2005) overloads the user and leads to '*password fatigue'* (Jøsang, Zomai, & Suriadi, 2007). Password fatigue is the negative feeling experienced when users must manage an excessive number of passwords. Not only does this affect users cognitively by imposing a heavy memory burden; it also compromises security as users often adopt disadvantageous strategies of password management, for instance writing passwords down or using the same login details for multiple accounts (Adams & Sasse, 1999). Conflictingly, passwords nevertheless remain the most common mechanism of validating an individual's credentials (Bonneau & Preibusch, 2010). As password login is an established and trusted ritual for users, introducing other mechanisms for identification, e.g. smart cards, may reduce familiarity and ease of use (Bonneau & Preibusch, 2010). Moreover, it is likely that previous experiences with security issues affect how users approach the login process: experiencing few problems in the past increases users' trust in the system (Bubas, Orehovacki, & Konecki, 2008).

2.2.2. Identity Management

Identity management optimisation is important in order to address the problems of managing multiple user accounts. IDMS typically have three parties: a user requests a service from a relying party (RP), which relies on the identity provider (IdP) to provide authenticating information about the user (Alpár et al., 2011). As with the identity construct, however, IDMS are not straightforward. Bauer, Meints and Hansen (2005) (in: Future of IDentity in the Information Society Project (FIDIS) , 2005) describe three types of IDMS: Type 1 for access control via authentication, authorisation[2], and account management; Type 2 for profiling the customer data of an SP for behavioural analysis; and Type 3 for users themselves to manage their digital identities and pseudonyms. Thus, IDMS are not merely a means for individuals to gain access control to services provided by organisations (Type 1), but also a means for organisations to inform their policies and decision-making (Type 2) (Rahaman, 2012). Therefore, beyond improving usability, functionality, and security, IDMS are fundamental in facilitating trust

[2] Authorisation: following successful authentication of the user's identifiers and credentials, the system retrieves the permissions of access attached to the user's identity (Rahaman, 2012).

relationships between individuals, organisations, and policy makers (Damiani et al., 2003).

To facilitate these relationships, technology implementation must have the user in mind. Criticising the traditional technology-centric perspective on IDMS design, Cameron (2005) suggested a user-centred approach of developing an identity metasystem, in which the usability problems of interacting with multiple, isolated identity systems are resolved by making these systems interoperable across multiple platforms and SPs. Cameron developed '7 Laws of Identity' to achieve this:

1. **User Control and Consent**
2. **Minimal Disclosure for a Constrained Use**
3. **Justifiable Parties**
4. **Directed Identity**
5. **Pluralism of Operators and Technologies**
6. **Human Integration**
7. **Consistent Experience Across Context**

However, these 'laws' were considered too simplistic and thus challenged by Dhamija & Dusseault (2008), who outlined '7 Flaws of Identity Management':

1. **Identity management is not a goal in itself –** rather, users are preoccupied with and motivated by their task with the service.
2. **Users follow the path of least resistance** – i.e. they will avoid taking any extra measures than they already do, even if security is improved.

3. **Cognitive capability is as important as technological scalability** – this refers to the cognitive burden of managing login credentials for multiple accounts.
4. **User consent leads to maximum information disclosure** – as users are not security experts, they often do not know what they consent to.
5. **We need mutual authentication (not just user authentication)** – to maintain security and prevent phishing attacks, users must be able to authenticate the IdP and RP.
6. **RPs want to control the customer experience** – and may therefore have reservations against cooperating with other IDMS.
7. **Trust must be earned (and is hard for users to evaluate)**

2.2.3. Federated Identity Management Systems

To accommodate the above guidelines, 'federated identity' is increasingly regarded as a feasible solution to user-centred identity management. Maler & Reed (2008) describes federated identity as the distributed storage of a user's aggregated identifying information, across multiple independent IDMS.

A FIDMS is defined by Jøsang & Pope (2005) as '*a set of agreements, standards, and technologies that enable a group of service providers to recognise user identifiers and entitlements from other service providers within a federated domain.*' This implies that users can access several independent SPs via a single IdP, provided the SPSs and IdP are members of the same federation, or 'circle of trust' (CoT). There are several benefits to this: FIDMS is superior to isolated identity models (Figure 2), for which the SP and IdP are the same, thus requiring users to adhere to a separate security-centric login policy for each SP they interact with (Flórencio & Herley, 2010). Instead, FIDMS leverages the same identifiers across multiple SPs (Dhamija & Dusseault, 2008). Moreover, as several IdPs can belong to the same CoTs (Figure 2), it overcomes the security problem of centralising all identifying information in the database of a single provider (Alpár et al., 2011; Rahaman, 2012). Finally, Liberty Alliance, a collaboration between several multinational organisations spanning numerous industries, is developing open standards for FIDMS, building on Oasis's Open Standard Security Assertion Markup Language (SAML) (Wilton, 2005), which may facilitate security, privacy protection, and seamless usability of FIDMS.

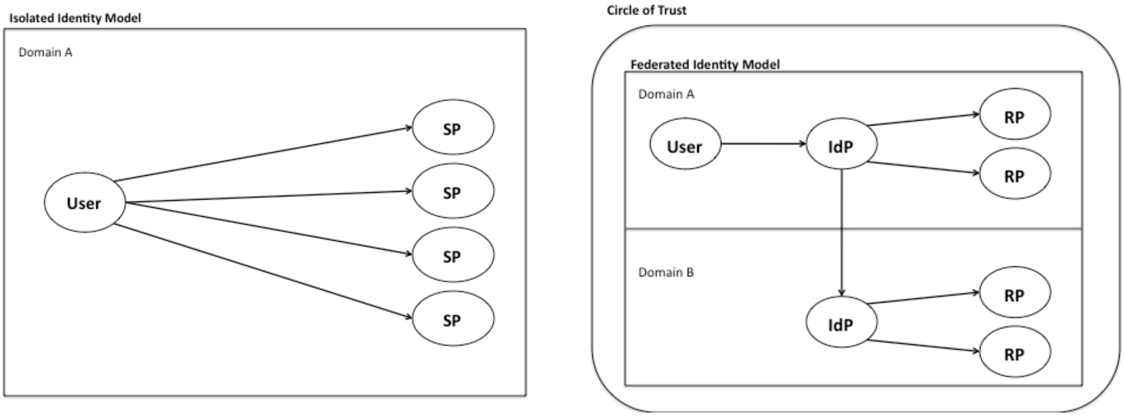

Figure 2. Isolated identity model: individual SPs act as individual IdPs, where the user goes through a separate log in process and maintains separate identification relationships with each SP in a specific domain. Federated identity model: several SPs act as RPs relying on the same IdP to authenticate a user within the same domain (A or B). IdPs in the same circle of trust (CoT) can exchange identifying information across the domains of use, such that the user can log in to use domain B services via a domain A IdP. Adapted from Alpár, Hoepman, and Siljee (2011).

There are several lessons to be learnt from existing FIDMS to bring forth in improving their user-centred design. An example of FIDMS is national education and research federations based on Athens and Shibboleth, which are single sign-on (SSO) systems allowing users to sign in via their organisation (often their university) to access several academic SPs (Chadwick, 2008). Other prominent examples are Microsoft Passport and

OpenID. Microsoft Passport allows users to sign in to several participating services using a single username and password created via their email address. While alleviating the burden of remembering multiple login details, it was criticised for giving Microsoft excessive control over users' personal information (Chadwick, 2008; McKenzie et al., 2008) and for being functionally limited and too centralised (Damiani et al., 2003). OpenID allows users to log in to SPs via a participating URL (Uniform Resource Locator), e.g. www.livejournal.com. However, a usability study found that users were confused when the login form violated their expectations by asking for a username but not password (Yahoo! Inc, 2008). Furthermore, the proliferation of URLs as IdP candidates is cognitively burdening (Dhamija & Dusseault, 2008) as well as challenging to associate as personal identifiers (Dhamija, Tygar, & Hearst, 2006). An attempt to address the existing problems with FIDMS are Google's four guidelines for FIDMS design: i) design for usability; ii) leverage what users already know; iii) design for widespread adoption; iv) allow for gradual migration (Google Inc., 2008). These are limited in their vagueness and do not appropriately address the user-centred issues preventing widespread adoption of FIDMS.

2.3. Identity in eGovernment

eGovernment, i.e. the provision of public sector services via the Internet, is a domain that is increasingly developing schemes for FIDMS implementation. The need arises from the fact that individuals interact with the government through various, separate channels (Baldoni, 2012). This requires users to maintain partial identities with each government agency, e.g. one for the tax department, one for the healthcare providers, and so on (Rahaman, 2012). Beyond providing services and benefits over the Internet, an ambition of eGovernment is to develop a '*joined-up government'*, where the fragmented interactions with public sector services are replaced with a seamless interaction and more coordinated information sharing between individuals and agencies (Pollitt, 2003). This may enable individuals to become empowered actors – not passive citizens – in controlling their lives as members of society (Mäkinen, 2006).

Further benefits of eGovernment include efficiency, reduction of administration costs, and national security. For instance, several governments, such as the UK, believe implementing a national identity management system (N-IDMS) will help overcome terrorism (Lyon, 2007). N-IDMS are schemes with a centralised database of citizens' personal information, for which citizens are issued a unique identity number or card to interact with public sector and private organisations. Furthermore, the UK government has argued that such a system will reduce illegal immigration and identity fraud (Lyon, 2009).

There have been some attempts of FIDMS for eGovernment, from which lessons can be learnt. The UK government introduced in 2010 a National Identity Card scheme with identity cards holding personal information such as biometric data. Due to substantial public disapproval citing injustice against civil liberties, the scheme was scrapped in early 2011 (BBC, 2010). The Austrian government implemented the Austrian Citizen Card, allowing for electronic identification and signatures for eGovernment services (Arora, 2008). Although deemed highly flexible and interoperable, its adoption rate was only 0.9% of the Austrian population (Sokolov, 2006). This was attributed to the cost and complexity of using the card, and the lack of benefit from using it from users' perspectives. Moreover, successful attack scenarios have been identified (Nentwich, Kirda, & Kruegel, 2006). This reinforces the need to consider human factors in developing IMDS. The UK Government Gateway is another attempt of an eGovernment FIDMS. Following registration to the Gateway, individuals can use the same login credentials to access over 100 services from more than 50 government offices, either through Gateway, Directgov.uk (the UK Central Government Portal) or via the specific government office's website (Lips & Pang, 2008). However, a one-off 12-digit alphanumeric password must be sent to the user's physical address every time a specific account needs inauguration (Office of the eEnvoy, 2002). Arguably, this disrupts the intended seamlessness of the system.

Moreover, the impact of private sector involvement in eGovernment must be firmly established to ensure the integrity of the system. A beta version of another centralised UK government portal was launched in 2011 at www.gov.uk (The Telegraph, 2011). Notably, the government is collaborating with private companies with existing databases of verified personal consumer information, such as VISA, for reliable user identification. The perceived benefits of this for FIDMS echo those discussed above. Further to this, privacy campaigners are less likely to protest against the collection of citizen data, as the government is relieved from this given the existing identity databases used (The Telegraph, 2011). Another issue with private sector involvement is that users can simply avoid using a commercial service they dislike. If users have an essential need to use a government service, however, they cannot avoid using it if they dislike it (McKenzie et al., 2008). This implies that greater transparency and higher accountability in terms of privacy and security are expected from government services (McKenzie et al., 2008; Camp 2004b). If government services are federated, however, diffusion of responsibility may arise: owing to the interdependence that federation introduces (Ellison, 2002), it becomes ambiguous which government level or agency is to blame for any system failures (McKenzie et al., 2008).

It is tempting to assume similar considerations should be made in developing both government and private sector IDMS (McKenzie et al., 2008). Indeed, governments and private companies are increasingly cooperating in service provision, for example by using third party companies as providers of digital certificates – i.e. encrypted software embedded in a PC's smart card or hard drive (eDT, 2005) in eGovernment (Lips & Pang, 2008). However, eGovernment inherently concerns itself with significantly broader issues of social inclusion, consistency, and interoperability, compared to commercial online services, which are not obligated to serve the entire population (McKenzie et al., 2008). To maintain the integrity of government, therefore, it is essential that eGovernment FIDMS promote the same fundamental principles as physical government in terms of universal and equal service access, fair treatment, and service outcome (Lips & Pang, 2008).

Finally and crucially, what users think of eGovernment is important to address. A recent survey by Accenture revealed key user concerns: although the majority of respondents use and appreciate online portals for interacting with the government, and support the increase of online government channels, one third of respondents were concerned about the government having too much of their personal information (ComputerWorld UK, 2012). This survey was limited to 200 respondents, however. User perceptions may also be heavily influenced by culture: Scandinavian governments have implemented various eGovernment FIDMS without putting particular emphasis on privacy or user control, e.g. Norway's MyPage. This has not resulted in the same public outcry and resistance as compared to FIDMS in governments in the UK and US (McKenzie et al., 2008). Presumably, long-lasting traditions of government openness in terms of e.g. freedom of information laws have fostered more trust in government in certain cultures compared to others (McKenzie et al., 2008). Social policies can therefore be of equal importance as technological implementation in facilitating user uptake of eGovernment FIDMS.

2.4. The Lived Experience of Identity

Crucially, there has been limited progress in understanding and addressing human factors and the underlying identity concerns of the *user* (Rahaman & Sasse, 2011). Digital identity research is predominantly technology-centred, i.e. '*almost exclusively tackled from within a technical domain by experts with a dominant background in a technical discipline'* (Lips, Taylor, & Organ, 2005). Traditionally, identity research is addressing the goals of the organisation in terms of their collection of personal data and surveillance of users, rather than evaluating digital identity and IDMS in how they impact users' interactions with organisations and the '*larger identity ecosystem'* (Rahaman, 2012). Moreover, identity management conceptions are limited to generic technological aspects, rather than address the specific role of citizen-government relationships in society (Lips & Pang, 2008). There is encouragement for a user-centred approach that does not merely investigate the usability of the technology, but also the relationship between digital identity and the individual, the effects of use of identity on the individual and their daily life, and both the static and dynamic components of identity (Cranor & Reagle, 1998; Rahaman, 2012). In other words, '*the lived experience'* of identity must be understood in order to develop a more fundamental user-centred perspective on digital identity management (Rahaman & Sasse, 2011).

While focus groups and individual interviews on perceptions towards N-IDMS have been conducted (Rahaman, 2012), there is very limited research in observing actual behaviour *in situ* for the use of existing public sector IDMS in daily life. This limitation is fundamental to address to reveal nuanced aspects of interactions with eGovernment, such as user intentions, coping mechanisms, implicit behaviour, and the dynamic nature of the interaction as it unfolds and fits into the overall context of everyday life.

2.5. Research Questions

To summarise, this literature review provided the context of digital identity, identity management of multiple user accounts, and federated identity for eGovernment. The lack of understanding of the *lived experience* for users in interacting with their digital identities and government services was highlighted as the main research gap in optimising user-centred FIDMS development.

Thus, there is a need to identify and develop a *user-centred* framework of the relationship an individual has to their digital identities, the identity system, the implementing organisation, and to society at large. The scope of the investigation is constrained to digital identity for UK eGovernment, and thus excludes areas such as eCommerce and social networking sites. This is because the literature review highlighted government’s distinctive role of encompassing broader issues, such as social inclusion. However, that does not preclude conclusions from this study to be applicable to IDMS beyond eGovernment.

Addressing the limitations of technology-centric perspectives of identity management, the present study will explore user perspectives of digital identity and eGovernment, as well as their actual behaviour as they interact with their digital identities for public sector services. The research questions are the following:

1. *Describe the relationship between the individual and their digital identity in eGovernment*
    a. How do users of eGovernment services perceive their digital identity?
    b. What factors influence their perceptions of their digital identity?
2. *Describe the nature of the daily life experience of interacting with eGovernment*
    a. How do users of eGovernment services interact with multiple user accounts in daily life?
    b. What factors influence the nature of their interactions?
3. *Identify implications for the design of a FIDMS for eGovernment*
    a. How do users experience current implementations of eGovernment services and federated identity systems, and how can this inform eGovernment FIDMS design?
    b. What are the factors and concerns influencing users' perceptions of a FIDMS for eGovernment services, and how can this inform eGovernment FIDMS design?

CHAPTER 3 **METHODOLOGY**

The following chapter describes a study addressing the research aims and questions introduced above. This includes the qualitative research methods utilised to collect and analyse the data, the participant recruitment process, and the study procedure. Overall, the study had three main phases involving participants: an initial interview, a two-week video diary study, and a final interview. This was followed by a final phase of data analysis.

3.1. Design

Addressing the research questions entails studying the rich and complex nature of behaviour surrounding user accounts in users' daily lives, as well as gauging users' attitudes and perceptions. Traditionally in HCI, quantitative approaches such as controlled laboratory studies and questionnaires are used to answer specific questions regarding interactions with technology (Rahaman, 2012). Such an approach was deemed inappropriate for the present study due to the ill-defined nature of the subject at hand and the contextual factors involved. Rather, an exploratory qualitative approach was taken, as it is regarded more suitable for poorly understood and complex socio-technical phenomena (Adams, Lunt, & Cairns, 2008). The findings from such a study can then form the basis for further and more well defined research (Sasse, 1997).

3.1.1. Semi-Structured Interviews

Interviews are an established HCI data gathering technique, effective at exploring rich and complex topics. Semi-structured interviews were decided upon for data collection, to strike a balance between serendipitous capture of interesting topics raised during interviews; and focusing the discussion on the broad concepts at hand (Berg, 2001).

Two main interviews were conducted with each participant. The first interview aimed at understanding how they reflect on their use of multiple user accounts, digital identity, and eGovernment services, and was conducted at the beginning of the study. This interview was largely similar for all participants. However, as the study progressed, new phenomena were captured during interviews, which led to additions to the question set for subsequent participants. See Appendix E for the question set representing the general topics addressed in each interview. It should be noted that each interview evolved slightly differently for each individual participant.

The second main interview was conducted after completion of the video diary, aiming to create a discussion between researcher and participant regarding key segments of their diary. For instance, it was explored what made the participant decide to interact with an online account at any particular time and place, and how they dealt with unsuccessful attempts at the task they intended to perform with an account. This second main interview was thus tailored to each participant and their respective diaries. Topics of interest that had surfaced in other participants' interviews or diaries were also discussed.

Additionally, a short interview was conducted midway through the video diary study, focusing on understanding how the participants found the experience of recording the video diary, e.g. whether the diary significantly changed how they would otherwise interact with the online account. This also provided participants with a chance to ask any questions they had, as well as a reminder to maintain the diary.

3.1.2. Video Diary Study

In order to verify the findings from the first interview, a two-week video diary study was conducted with the same participants. This aimed to reveal any observable phenomena difficult to overtly discuss retrospectively in interviews. Drawing on contextual inquiry methods (Beyer & Holtzblatt, 1997), its purpose was to understand and explore naturalistic behaviour as it dynamically unfolds over a longer period of time. As the use of video diaries is unestablished and relatively novel in HCI research, this subsection will outline the rationale behind this choice for data collection.

Video diaries have been used to capture what participants would have envisioned their behaviour to be with future technology (Jones et al., 2011). It has also been used as an HCI research method by Kamsin, Blandford and Cox (2012) to explore *actual* behaviour as it unfolds. These researchers equipped participants with Flip cameras to record diary entries of their everyday experience and behaviour regarding academic task management. A one-month video diary study of users recording their experience with OpenID was conducted (Kakali, 2010), however this focused mainly on the interaction with the interface, evaluating its functionality, rather than the daily life experience aspects of OpenID.

While video diaries are novel, diary studies in general are widely considered to successfully balance the need for empirical support of conclusions with unbiased experience from users' point of view, by having participants themselves record data (Carter & Mankoff, 2005). Diary studies are a type of *elicitation study*, i.e. entail having participants self-initiate media caption of the event and their behaviour, to act as cues for subsequent interview discussion with the researcher (Carter & Mankoff, 2005). Grawemeyer and Johnson (2011) conducted a one-week written diary study of multiple passwords management, revealing rich and naturalistic data of different password strategies and password-service relationships.

Video diary studies have several methodological advantages: participants are not distracted away from their task or biased by study expectations; and they may capture *intentions* to use an account in the absence of successful execution. This latter aspect may rarely be mentioned in self-report, highlighting a key advantage above interviews. Moreover, self-initiated data collection highlights what experiences and behaviours participants themselves choose to highlight. Also, it has been established that event prompts such as captured media improve people's episodic memory of the event (Barsalou, 1988; Carter & Mankoff, 2005). Finally, conducting the study over two weeks is likely to allow for exploration of dynamic phenomena that change over time due to factors external to the identity system itself.

3.1.3. Grounded Theory

The data collected from the interviews and video diaries were transcribed in full and analysed using the Grounded Theory (GT) method (Strauss & Corbin, 1990). In contrast to the traditional scientific method of testing previously postulated hypotheses and tested theories (Popper, 1959), GT adopts a bottom-up, exploratory approach to building a theory emergent from the data. A key aspect of GT used in the present study, is the continuous cycle of data collection and analysis until a point of information saturation was reached: the first participants generated new topics of discussion which were introduced to subsequent participants, until new topics ceased to appear. It was important to conduct interviews and video diaries on a rolling basis, allowing any new discoveries to be addressed for subsequent participants, and for initial coding to be refined iteratively.

The transcripts were printed and coded according to the three stages outlined by Strauss and Corbin (1990):

- *Open coding:* beginning with the GT principle that '*all is data'* (Strauss & Corbin, 1990), the full interview and video diary protocols were reviewed to extract discrete situations, perceptions, and topics discussed. Similar extractions were grouped into concepts. Example: an extracted concept would be a participant's reflections of whether they trusted the login process to access an account.
- *Axial coding:* the concepts were assembled and links were established between related concepts in order to identify how the concepts were connected. Example: an identified connection was that between participants' trust in the service

organisation contra their trust in the technology supporting the organisation's online services.

- *Selective coding:* core categories of concepts were identified, around which narratives were developed in order to support the emergent theory. Example: a narrative around the core category of 'interacting with the organisation' was developed, whereby it was found that participants relate differently to an organisation's intent of data protection and the security of an organisation's technology.

See Appendix G for examples of transcripts from interviews and video diaries.

3.2. Participants

Fifteen participants were recruited (Table 1). Seven participants were UK nationals; seven participants were overseas nationals who had lived in the UK for study and work purposes for at least six years; and one participant (P7) was an overseas student who had lived in the UK for the past year. All participants were based in the Greater London area at the time of the study. In meeting the recruitment criteria, all participants used at least three public sector accounts, and accessed several of them at least once over a two-week period. A £50 Amazon® gift voucher was awarded to participants at completion of their participation.

Table 1
Overview of participants

Participant Code	Age	Gender	Academic/Professional Field
P1	22	F	Psychology; Social & Public Communication
P2	21	F	Geography
P3	20	M	Italian; Geography
P4	21	M	Space Science & Engineering
P5	20	F	Electrical Engineering
P6	24	F	Psychology; Assistant Psychologist
P7	23	M	Oncology
P8	22	F	Neuroscience
P9	19	F	Biological Sciences
P10	26	M	Pharmacogenetics & Stratified Medicine
P11	22	F	Digital Marketing
P12	20	F	Neuroscience
P13	24	M	Social Cognition
P14	23	F	Social Cognition
P15	24	F	Cognitive & Decision Sciences

3.2.1. Recruitment Questionnaire

Participants were recruited via an online questionnaire distributed to the researcher's wider social circle and university (Appendix A). The rationale behind constraining sampling to this population was that individuals connected to the researcher and/or the university would be more likely to participate, and more comfortable participating due to the nature of the information to be disclosed.

The initial purpose of the questionnaire was to select participants according to the services used, to ensure an adequate variety of services, level of frequency of use and experience of use. It also aimed to ensure a variety of educational and occupational backgrounds.

Another initial purpose of the questionnaire was to filter out participants likely to be dishonest about their interactions with user accounts. A 10-item version of a Big Five personality inventory (Costa & McCrae, 1992) was included. The Big Five framework has received substantial empirical validation, wide use and support by behavioural researchers (Gosling, Rentfrow, & Swann, 2003). As the full inventory has 50 items, a short version was used to relieve the burden for participants. The shortened inventory has been found to reach adequate levels of empirical validity, such as test-retest reliability and external correlates (Gosling et al., 2003). High scores on Agreeableness and Conscientiousness, and low scores on Neuroticism have been found to be associated with high integrity (Ones, Viswesvaran, & Schmidt, 1993). By selecting high integrity participants, it was hoped that the study would exclude participants with the propensity to be dishonest about their use of online accounts.

The questionnaire did not gain sufficient responses for substantial filtering to occur, as only 10 individuals responded, of which nine qualified in terms of the type and number of online accounts used. There may be several reasons for this: as the study was conducted over the summer months, most of the researcher's social circle were on holiday or too preoccupied with research projects of their own to be able to commit to a two-week study. Furthermore, the sample population is unlikely to use as many government services as for instance an older, non-university population. Hence, due to the sampling method and perhaps the characteristics of individuals likely to volunteer to participate, e.g. students attracted to the monetary incentive, the resultant participant sample of young, academic Londoners was not as varied as initially desired. Ultimately, the questionnaire fulfilled the purpose of generating a rough participant profile prior to the study proper. Moreover, the homogeneous nature of the participant sample advantageously allowed for comparisons of phenomena revealed by individuals.

Using the scoring method according to Gosling et al. (2003), it was found that 14 participants scored highly, whilst one participant (P13) scored medium on Openness to Experience. No other patterns were found for the remaining personality traits.

3.2.2. Selecting Online Accounts

It was difficult to determine which online services to include (Table 2) for participation, in particular due to the heterogeneity of government influence in public sector organisations. It was expected that participants would be unlikely to treat government-owned for-profit corporations, such as the Royal Mail, in a similar manner as they would treat not-for-profit government services, such as the Driver and Vehicle Licensing Agency (DVLA) and HMRC. This was also the case for for-profit organisations in which the government has either full or partial ownership, such as East Coast Trains and The Royal Bank of Scotland Group. Owing to individual variability in participants' perceptions of government influence in for-profit organisations, it was decided to leave their inclusion at the participants' discretion. Some participants had several reflections regarding the government-related aspects of using such services, while others were unaware of the government influence, believing they were entirely private.

It was further decided to include university intranets and national research databases. This was for the purpose of exploring participants' use of existing SSO systems, such as Shibboleth, which could be beneficial for developing design implications for a FIDMS for eGovernment. Additionally, some participants expressed reflections concerning government influence in public universities, e.g. public funding in academia, which were deemed relevant for the study.

Table 2
Overview of online accounts

Online Account Type	No. of Total Logins Over 2 Weeks	No. of Participants with Account
University Intranet	28	13
National Research Databases*	0	3
Student Finance	2	6
Banks (RBS, Lloyds TSB)	2	2
Transport for London (TfL)	17	11
East Coast Trains	5	3
The NHS	4	3
Armed Forces	2	1
Local Council Authorities	5	4
The DVLA	0	3
Jobcentre Plus	0	1
London 2012	1	2
The HMRC	0	2

* 'National Research Databases' include EDINA DigiMaps and the NHS NIHR (National Institute for Health Research).

The flexibility with regards to which online accounts to include had several advantages. Firstly, it would be unlikely that participants would use direct government services, such as DVLA and HMRC, on numerous occasions over a two-week period. This was because these services are more likely to be used on a monthly or yearly basis due the non-routine nature of their associated tasks, e.g. paying car tax. Limiting focus to only these services could potentially bias participants towards using them more often than they otherwise would, for the purpose of the study. Secondly, it allowed for exploration of a broader range of issues surrounding the use of multiple accounts, beyond the strictly government service aspects, and allowed for comparisons between different types of services.

3.3. Procedure

The majority of the interviews were conducted in study rooms at University College London, while some were conducted in the participant's home at their discretion.

Participants were first informed about the study via verbal instructions (Appendix D) and a written information sheet (Appendix C), and then given a consent form to sign (Appendix B). The first interview was then conducted, asking questions concerning their general online account use, their use of public sector services offline and online, their perceptions of government organisations in general, and their perceptions of their digital identity, online presence, and personal information. Each interview was audio recorded, and lasted for approximately 30-45 minutes.

Participants were then given a Flip Video Mino recorder to produce the video diary. They were given a brief demonstration of its use along with a sheet of suggestive instructions (Appendix F). It was emphasised that the instructions sheet was for general guidance only, and that it was ultimately at the participant's discretion how they preferred to record their entries. For instance, filming their talking head versus their computer screen, and filming in real-time versus immediately after the interaction was stressed to be up to the individual participant. It was further stressed that it was important that the interaction was naturalistic and non-forced, and that it was up to the individual participant what type of and how much information they wished to disclose. These unconstrained instructions were beneficial in capturing naturalistic behaviour, and in ensuring that the making of the diary was comfortable for participants.

Each participant recorded entries of their diaries for two weeks. During the two weeks, the short follow-up interview was conducted, either in person, via phone, or via email. Participants were also asked to send the first one or two recordings to the researcher via Dropbox[3] to ensure they were on the right track.

At the end of the two weeks, the participant met with the researcher for the debriefing interview. This was also audio recorded and lasted for approximately 30-40 minutes. Finally, participants were paid and thanked for their participation.

[3] Dropbox is a file sharing service that allows storage and syncrhonisation of files across computers. It is operated by Dropbox, Inc.

CHAPTER 4 **RESULTS**

This chapter presents the main findings of the GT analysis of the collected data, an overview of which can be found in Table 3. Three main themes emerged, each with a subset of related categories:

- *Levels of Interaction:* participants interacted with eGovernment identity and accounts on different levels. These emerged in analysis as individual, technological, organisational, societal, and ethical levels.
- *Contexts of Interaction:* participants interacted with eGovernment identity and accounts in a variety of contexts. These contexts emerged in analysis as three categories, namely a task/purpose context, a location/device context, and a time/life situation context.
- *Perceptions of FIDMS:* participants expressed their perceptions of FIDMS from two perspectives, namely by evaluating their current experience of multiple separated accounts, and by considering hypothetically federated accounts.

All 15 participants successfully completed the study. The number of video diary entries submitted ranged from four to nine, with an average of six per participant. The length of entries ranged from 1 min. 28 s. to 36 min. 46 s. A single entry includes interrupted account login sessions, and sessions with several logins to different accounts. The analysis reflects data from the interviews and video diaries combined.

Table 3

Overview of the findings from Grounded Theory of qualitative data

Theme	Category	Description
Levels of Interaction	*Individual*	Behaviours and perceptions of individuals' own personal information; how they define identity/digital identity; how they decompose their identifying information; and how they compare and value different manifestations of identity.
	Technological	Behaviours and perceptions of digital identity systems; interactions with online accounts; security; privacy; trust; the distributed representation of personal information online; and the differences between digital and physical authentication processes.
	Organisational	Behaviours and perceptions towards identity in relation to the overarching organisations providing the benefits and services individuals use, including different levels of trust in government versus non-government organisations.
	Societal	Behaviours and perceptions towards the role of digital identity in society, including how it might be used for national security and population surveys.
	Ethical	Ethical perspectives on digital identities; the sharing and misuse of personal information online; individual rights to privacy protection; and individual versus legal responsibility of online activities.
Contexts of Interaction	*Task & Purpose*	Behaviours and conditions related to the intended task with the service, including perceived benefits; any interaction prompts; coping strategies; and how interactions occur.
	Location & Device	Physical contexts of interacting with services, including where and on what devices the interaction occurs; and how the interaction is affected by reliance on physical artefacts.
	Time & Life Situation	Temporal factors influencing the interaction, including the effects of time pressure on interactions; for how long interactions last; and how changes either during the interaction or in users' lives affect the interaction.
Perceptions of FIDMS	*Multiple Separated Accounts*	Perceived strengths, limitations, and any key issues and problems experienced while interacting with multiple separated user accounts.
	Federated Accounts	Perceived strengths and limitations of a hypothetical eGovernment FIDMS; and any key issues and problems experienced while interacting with existing IDMS.

4.1. Levels of Interaction

4.1.1. Individual

Participants did not perceive their identity with government services as representing their individual person, but rather as representing them as part of the population data:

P3_interview: "Not as a person; as another thing on the database, but not a true identity as an individual. (...) You're just part of a list of numbers."

P12_interview: "They're just your data, really. Just like the raw, quantitative details of your existence, that's just what I think a digital identity is."

Further to this, participants perceived a division between an 'official identity' and a 'personality identity', the former being the one used with in eGovernment, and the latter being the one used in for instance social networks. Official identity was considered more permanent, externally generated, and important for people to uniquely identify them, but not consciously related to on an everyday basis. Contrastingly, personality identity was considered more impermanent and flexible, internally generated, and the identity consciously related to on an everyday basis:

P1_interview: [about official identity] *"I think it's more of an awareness, you never think about those things, you see that as something that you* have *to have, like passports. (...) So that identity is something created externally, I think, like your credit score, you're not born with that."*

P3_interview: "It's [official identity] *not something I think about, it only comes up when you need to use it. (...) It's an official thing for using, well, official things. Like* *carrying my driving licences, but it doesn't feel like an actual driving license unless I'm actually going to drive somewhere."*

P12_interview: "I think the actual person of me is my personality (...) 'cause you can change your name, you can change your address."

Participants personally valued their personality identity higher, as it was considered a larger emotional investment, and thus more vulnerable on an affective level. Simultaneously, they acknowledged that their official identity information would be more vulnerable security-wise:

P3_interview: "If some hackers could see my logging into Portico, blood donation website or my Student Finance account, I would be much more aggrieved than if they were able to see my Facebook or Flickr."

P5_interview: If they sort of saw you in a social network, and they knew you're funny and you like going on holidays, they couldn't use that against you, but they could use your address and things like that against you. So for me, that's more important."

4.1.2. Technological

Participants perceived user accounts as identity facets. P3 reflected on how contextual boundaries, e.g. the information required to disclose to access a service, defined a facet. He also perceived all facets to inherently be part of the same identity:

P3_interview: "Some might be more restrictive or sort of confined to different boundaries, but if there was no boundaries anywhere, it probably wouldn't differ across things. But it would still be a difference because of boundaries that will just constrain things."

Most other participants also perceived the aggregation of their identity facets to constitute their overall digital identity. Moreover, they perceived individual facets to represent individual relationships to each SP – for example:

P9_interview: "Like there's an identity for the DVLA commune, an identity for the library commune, sort of like aspects of a community. So you're part of each one and can sort of link them as a web identity with each other, in a way."

Most participants felt they gave up control of their identifying information once they submitted it to SPs:

P3_interview: "I still consider it mine, but I wouldn't consider it controllable in the sense that once it's gone into the sort of database somewhere, it's there."

P12_interview: "I feel like the company, it's their *website,* they *have my accounts. So I guess the data itself is mine, but I don't feel like I have any ownership really."*

P13_interview: "If they wanted to know they can easily know everything, I mean, it's their *system I'm using."*

Prior experiences with security problems, or the lack thereof, had a significant influence on participants' subsequent behaviour and attitude towards protecting their identifying information. Since most participants had not experienced identity theft or similar before, they were not particularly concerned with security. However, several participants – for example P3 – expressed an awareness of perceived versus actual security, mediated by their perception of the organisation

P3_video: "It says that 'we are securely *logged in', but anything can say you're securely logged in, so that's not reassuring really. But it's more a combination of* that *alongside trusting it* as *an organisation that has a considerable part of it that is owned by the government."*

While most participants were aware that their online activity was recorded by SPs – P3, P5, and P12 providing concrete personal examples of targeted advertising and cookie policies – they did not believe their individual activity with government-related accounts was subject to targeted monitoring. Several participants reflected on the implications of storage of location-based information in, particularly in Oyster card accounts, but were not concerned that it would be misused – for example:

P4_video: "… that account not only is tied to my bank account for paying of travelcards and top-ups and stuff, but also has a photo of me, details about my university and so forth. And on top of that it has, you know, my journey history of where I've been in London over the last, I don't know, month or longer. I'm not worried about it, but I can see how some would."

In comparing using online versions of public sector services with physical interactions, participants believed that identifying themselves physically was more certain than when online. For instance, P4 perceived digital identification to only prove that an individual holds an account, while P10 reflected on how digital information can – unbeknownst to the IdP – be shared between individuals:

P4_interview: "You can prove that you're the holder of whatever account with your password or secret word or whatever. But proving that it's actually you *as opposed to just a person is a little complicated."*

P10_interview: "I can give my user-ID and password to a friend and they can login whenever, but a passport, they can't."

4.1.3. Organisational

While participants did have some trust concerns regarding the security of the interface technology, most participants did inherently trust the overarching organisation:

P4_interview: "I'm not worried about the government knowing *my information; I might question their ability to keep it securely given things recently. (...) I'm fairly trusting when it comes to* intent.*"*

P11_interview: "For government organisations, it's an external *factor, so it's not the people I don't trust, but the security systems around it."*

Moreover, most participants trusted government-related organisations, including government-owned enterprises, more than private, profit-driven organisations. This was because they believed they derived higher overall benefit from a government organisation, and that government-ownership introduced more reassurance and accountability with regards to security issues:

P3_video: [East Coast] *"Because it's government-owned, it gives you more confidence in its security (...) especially now that they actually have taxpayers' capital invested in it, so it's in their interest for it not to go bad or whatever in terms of security."*

Some participants reflected over government-owned enterprises. While this did not cause participants to trust these organisations significantly less, they did prefer the organisations to be transparent in their profit-driven agendas:

P3_video: "It's almost as if Royal Mail deliberately misleads people into being public while operating privately in order to gain more trust. I think people trust Royal Mail more because it is *government-owned (...) Now unlike East Coast, there's no hiding it. (...) I don't see any problem with it as long as it's not sort of hidden."*

P8_interview: "When I first came to the UK, I thought it was very official, it's called 'Royal Mail', and then I realised it's just one of the companies. I think it's fine, but it's like a government thing but it's not really government like other things."

4.1.4. Societal

Participants saw the role of digital identity management as beneficial for society in terms of national security and for detecting suspicious behaviour. They were therefore willing to compromise their own privacy concerns to ensure higher levels of protection for everyone for pragmatic reasons. For example:

P1_interview: "I don't think it's the right thing to do, but in those circumstances, it's probably the easiest or quickest or safest way of handling things."

P10_interview: "This is sort of entering your privacy (...) But I'm the good guy, and there are some bad guys out there, so you have to make a balance to make society safer."

However, several participants expressed that even if the state increased their security levels, agents threatening national security would counter this by increasing their own technological sophistication. For example:

P1_interview: "They're [the government] *is just making the game play a little bit more difficult but more advanced as well. If you give the basic trust in the beginning, then the terrorists will use their minimum technology or whatever way to get around it, so you will make it easier to catch them as well."*

P4_interview: "It's sort of like, the better the identification, the more damaging it is if it gets compromised if someone else has access to that."

P7_interview: "You always see this arms race between people who are looking to protect data and people who are looking to try and gain access to it, legally or otherwise."

Participants saw the benefit of identity systems for population survey and statistical purposes in the interest of collective society. However, many stressed that while gathering of collective data was acceptable, they opposed being singled out individually – for example:

P1_interview: "I would assume the government is not targeting me *personally, but for the general population. So I don't take it too personally."*

P3_interview: "Being tracked as an individual is worse than being tracked as one of a crowd."

Participants were also accepting of collective monitoring as long as individual records were not aggregated, for instance as expressed by P8:

P8_interview: "If they make separate recordings of what I do, and they don't put it together as being a kind of identity that they think I *am based on what I'm doing, then that's fine. It's like in a store, then they have to videotape and it's fine, but it's not fine if they link that with some other security tape and try to figure out whatever I'm like."*

4.1.5. Ethical

The majority of participants perceived eGovernment services and their associated user accounts as a part of digitised society, and that similar ethical and moral rules as in physical society should apply:

P3_interview: "If it exists in normal life, so you're putting a lot of your normal life onto the Internet, then that privacy should be extended to that as well. (...) The Internet isn't some unreal world."

However, some participants, like P4, argued that this would be impossible to implement technologically:

P4_interview: "You can't enforce anything like that ever on the Internet (...) That's a bad thing to do, but you can never enforce that."

Contrastingly, P2 and P10 held the strong view that anything in the digital environment was exempt from the rest of society's ethical conduct. Accordingly, they had taken the liberty themselves to use other people's personal information online:

*P2_interview: "*Everything *online is fair game, the Internet is not private and you have to realise that, everyone does. And if people have a problem with taking their* *stuff, well, they put it all out there. (...) You can take everything from someone. I've done it before."*

P10_interview: "Nothing on the Internet is fair (...) Sometimes I hack some people's accounts as well. (...) This is a situation you create yourself, you know, if you pat that much information in your account, a person can easily identify you, and I think you have to be liable."

The issue of where the moral responsibility lies when personal information is out in the open was emphasised. While participants agreed that there should be proper legislation in place to protect individuals' privacy, they also acknowledged that some responsibility lies with the user:

P6_interview: "I think you have to use common sense in a way. If you give up personal information to something that looks dodgy, then I think you are to blame a little bit."

P9_interview: "I think there should be laws to protect people, but obviously if you put your stuff online, then you should expect the worst case scenario to be it might be shared. (...) So you should always be aware of the risk, I think."

4.2. Contexts of Interaction

4.2.1. Task & Purpose – What users do and how they do it

All participants initiated an interaction with a public sector service in order to complete straightforward, routine tasks that were necessary as part of their personal administration and everyday planning, such as checking that their Student Finance application was complete.

Registration and use of services was for the purpose of immediate need, rather than for perceived potential benefit. Most interactions were pragmatically driven, e.g. participants did not linger on the service to explore, but were motivated by concrete tasks, immediately ending the interaction once the task was completed or interrupted.

P4_video: "...you just want to get in and get out with the information you're looking for."

When participants failed to remember login details, experienced network or server problems, or simply did not know how to login, physical interaction with the service was necessary. Participants would report intending to complete the task offline, e.g. by phoning the service or visiting their physical location. However, when asked about this in follow-up interviews, none of the participants actually saw this through, blaming forgetfulness or lack of time.

Participants tended to interact with several related services in a same session: for instance, P3 recorded a lengthy session of interacting with Student Finance, student accommodation, and university Intranet; P12 recorded using her council library and university library in a session; and P4 recorded three entries of both Oyster Online and Barclays Bicycle Hire together:

P4_interview: "You'll be in sort of like a personal admin mode, and think 'I'll do this and I'll do this' and then cross them off the list."

All participants agreed they preferred using public sector services online rather than offline due to the convenience, sense of personal control, self-reliance and empowerment it brings:

P5_interview: "It lets me know in advance and plan things, so that I can budget things as well, and I'm not wasting my time."

P7_interview: "In terms of the time invested, what I get out of doing things digitally is worth more than what I'm able to do physically in the same time."

P9_ interview: "You don't have to like travel all the way to your local council to like stand in millions of queues."

P10_interview: "It gives me more freedom, I don't have to carry money or ID with me, and I can do it whenever I want, midnight or whenever."

4.2.2. Location & Device – Physical contexts

Participants' interactions occurred at home in the evening, after having completed other activities for the day, or in between longer-lasting Internet activities, such as social networking and media. Thus, participants interacted when settled down in a physical location, rather than sporadically at various locations throughout the day. Home computers were the main device used.

Mobile devices, i.e. smartphones and tablets, were more frequently used while on the move. This tended to be for transportation services, such as checking one's Oyster balance. Mobile devices were used in the home when laptops were switched off: knowing the tasks would be brief and non-critical, participants frequently said it was not worthwhile taking the time to boot their computers. Apart from the smaller screen real estate, participants did not consider using mobile devices any more inconvenient compared to laptops.

Shared devices or public computers were reluctantly used due to privacy concerns:

P8_interview: "If I was in the same room as someone (...) were using my computer and they saw me, I don't know, like, I feel that there's intrusion on my privacy."

P10_interview: "I don't feel very comfortable when I do these things, so the best I can do is (...) use private browsing so no data is kept or stored in the system."

Furthermore, participants disliked interacting with services dependent on physical artefacts. P5, P9 and P12, in particular, found the username for their council libraries challenging to remember, and disliked the need for the physical library card whenever logging in. For example:

P5_video: "I need my card number and sometimes I don't know where I've put my card, so it's really annoying that I have to go downstairs and get my card number. It would be much easier if they changed it to a username, what it usually is."

Similarly, P3 and P12 reflected on having to keep paper documents detailing their customer login information for Student Finance, expressing frustration over the reliance on physical storage to aid memory:

P3_video: "I need to get my bit of paper, because to login to Student Finance, I need to use a customer reference number, and I would never *remember it, I forget it* all *the time. I have to keep this tatty piece of paper that I've had for…well, since the 27th of June 2011, so a year yesterday, this bit of paper."*

P12_video: "So Student Finance is notoriously horrible *to login to, and I have a box like this [films shoebox-sized box], and in this box I keep all my login details for this kind of thing. I can remember my password, but I can't for the life of me remember the 10-11-digit code to get in, so I just have it in this box, like…it helps. Because if you just keep it in scraps of paper, then you always lose them."*

4.2.3. Time & Life Situation – The effects of time and dynamics of life

Changes in participants' life situations caused short- and long-term changes in how they interacted with different services. P4 reflected over his temporarily increased use of TfL services due to an unresolved problem with his missing cycle hire key, and how the login process was facilitated accordingly. P6 and P11's life situations both changed in terms of starting a new job and losing a job, respectively, thus affecting the type and frequency of service interactions:

P6_interview: "I found also that because I'm now in a kind of a new stage of my life, I would use that [East Coast] more*, but then other things* less. *So for example I would be going to events more, I would be using East Coast more, but also using Oyster card less, because I would just have to book a day card all the time. So kind of my usage has changed, so there's less Royal Mail and more travel."*

P11_interview: "…'cause the past week I was made redundant, so I just look up stress and like psychological health and all that stuff, and if there's any kind of support service."

Participants experienced problems when life changes caused their identifying information to change, and this failed to synchronise with the identifying information in their user accounts. P8, for instance, experienced difficulties retrieving her Oyster account password, which required entering her postcode:

P8_interview: "I got really confused because I couldn't remember which postcode I left with them, because I moved three times."

Similarly, P3 and P12 reflected over how Student Finance relies on users to remember the identifying information initially linked to their account upon registration:

P3_video:"And that's annoying, when Gmail went available in the UK instead of Google Mail, then I didn't change everything to Gmail, so some things still had Google Mail on their records (...) Because obviously I did this in Sixth Form when I first signed up and I haven't changed much since then, so obviously it is the old Google Mail, or hopefully, obviously, I don't know. Maybe that's just a fail and I'll have to start all over again, or just not *do it."*

P12_video: "My brother got Student Finance in the first year that it was put into place, which is like 10 years ago. And my parents signed up for it 10 years later, when I used Student Finance, Directgov, the people that run this, expected my parents to remember their customer login and so on, which they had no idea, they didn't even know what email account they were using 10 years before."

Participants had a tolerance threshold for how much time and effort they invested in attempting to login and complete their task, mediated by factors such as their mood, the importance of completing the task, and the urgency of external influences, such as needing to leave the house. For example:

P11_interview: "If I'm pissed after a long day, I'll screw it. If not, if I really want the information, then I try for two or three times. (...) Also time pressure, so if I need to do something after, I'm just like never mind, let's do this quickly or screw it."

4.3. Perceptions of FIDMS

4.3.1. Multiple Separated Accounts

The main benefit of maintaining multiple, separate accounts, was the sense of control it gave participants in knowing what information was disclosed where, and preventing the different organisations from exchanging their information without their knowledge:

P1_interview: "I think every time you give out information on different websites, you sort of have this sense of control, you kind of know *how much information you want* this *provider to know, how much you want the other one to know. Is it all necessary or is it not necessary. (...) It's more about control, information control."*

However, participants experienced far more disadvantages of managing separate accounts, in particular the memory burden of maintaining multiple passwords. All participants developed coping strategies, such as using the same passwords for several accounts to the extent possible. Moreover, participants relied heavily on password retrieval procedures as the rule rather than the exception during the login process.

When different passwords were used, participants normally lacked any strong association between the unique password and the user account, thus engaged in trial and error behaviour from their known set of passwords across all user accounts:

P6_interview: "The way I manage it is, if I can't remember it, I just try the first, most complicated one, and if that doesn't work, I go down one step, and if that doesn't work, I try the last [laughs]. So it's not much managing, it's just…trial and error."

Observing participants' use of Shibboleth for research resources was insightful in terms of participants' experience of being redirected to different websites for logins. Notably, participants tended to get lost, leading to much frustration, confusion, and disruption of the interaction flow. Importantly, participants perceived the implementation of numerous site redirections to be unnecessarily challenging.

4.3.2. Federated Accounts

When asked about their perceptions of FIDMS for eGovernment, most participants agreed it would be far more convenient compared to separate logins. Additionally, several participants bemusedly said they believed government organisations already had all their personal information centralised, if not easily accessible:

P4_interview: "Ultimately, if someone really wants to find that information, they can, 'cause it's the government *[laughs]."*

In addition to not having to remember multiple sets of usernames and passwords, another perceived benefit was not having to resubmit the same personal information to several SPs, e.g. details of their student status, in order to prove their entitlement to a service or benefit.

Nevertheless, several participants stressed the importance of only allowing strictly relevant information to be exchanged amongst members of the federation:

P8_interview: "They have to make sure that they don't really use other information for other purposes, but they only use whatever they need *from my account."*

Many participants also questioned the technological implementation of a FIDMS in terms of the weakened security of having the same login details for several services:

P5_interview: "If I had one password for everything, that makes me more scared, because that means they can unlock my whole digital identity."

Some participants, like P9, raised concerns regarding the diffusion of responsibility in a FIDMS:

P9_interview: "If some suspicious money went into my account, if I had one login for like four services, it would be difficult to know who took the money. 'Cause they couldn't sort of go and blame each other, like saying, 'it wasn't me, check your *services.'"*

All participants were strongly against non-government third parties being included in the federation. P3 believed government-owned enterprises should be excluded as well, fearing the increased exposure to users would give them an unfair advantage over private enterprises. Participants expressed concerns about their personal information being misused for profit, perceiving a clear distinction between the purposes and agendas of public sector versus private organisations. For example:

P12_interview: "I think that would be really, really *strange if a private company did it, because that's like a different aspect of your life completely. Like the government* *things are things that you* need *to do, you* need *to use TfL, you* need *to get information from the NHS and pay your taxes and whatever, but social media and banking is like a completely different kettle of fish."*

Finally, several participants expressed concerns about having a same login for services they considered required different levels of security. For example, accounts involving financial transactions were considered to require higher levels of security, whereas accounts containing only basic demographic information were not. However, participants were apprehensive in deciding themselves what level of security is required for what service, due to insufficient technical knowledge.

CHAPTER 5 **DISCUSSION**

An exploratory, qualitative study was conducted using interviews and video diaries, investigating users' perceptions and experiences of digital identity, managing multiple eGovernment accounts, and attitudes towards federated identity systems for eGovernment. This chapter highlights main findings that emerged in the study, to be discussed in the context of the reviewed literature.

5.1. The Lived Experience of Identity

5.1.1. A User-Centred Perspective of Digital Identity

Participants did not perceive digital identity to be a single construct encompassing their entire person, but rather multifaceted and contextually dependent constructs. This supports the concept of multiple context-dependent partial identities (Damiani et al., 2003; Pfitzmann & Hansen, 2010). In particular, participants made a broad distinction between their official identity and their personality identity. Their official identity, used for eGovernment, generally consisted of variant identifiers, such as home address and customer reference numbers, which could be subject to change or removal. This conceptualisation of identity is in line with HCI literature, describing digital identifiers as dynamic and variant (Maler & Reed, 2008; Jøsang & Pope, 2005; Alpár et al., 2011). Moreover, it was frequently expressed that participants did not actively engage with their official identity on a daily basis – rather, it was only relevant and identified with when it was used to access a specific service or benefit. P7 called it *"a means to an* *end."* Thus, the official identity is not necessarily an identity *per se*, but an identity required for a specific situation (Cameron, 2005).

Contrastingly, the personality identity consisted of permanent or long-lasting identifiers, such as personality traits, values, and interests – identifiers that define who an individual is, how s/he is "*really* like*"* (P4). While this identity was valued higher by participants on an affective level, due to being the identity they related to on a daily basis in their interactions with others; participants were aware of the more serious consequences should their official identity information be compromised. They therefore stressed the importance of the protection of their official identity.

The user-perceived dichotomy of an official and a personality identity thus supports Durand's (2003) distinction between an assigned, context-dependent identity (Tier 2); and a personal, true and inner identity (Tier 1). Moreover, participants' perception of their eGovernment identity as an impersonal part of population statistics corresponds to Durand's Tier 3 identity, i.e. an abstracted, demographic-based identity. Other authors have made similar distinctions: Wharburton (2010) stresses that rather than being concrete concepts, facets of identity lie on a continuum: on one end is the 'narrow' digital identity, i.e. a collection of online credentials; and on the other end is the 'broad' digital identity, i.e. the personal self portrayed in social interactions. While it was not clear from the present data whether participants considered the dichotomy to be discrete or continuous, it provides an empirical basis subject to further study. Importantly, addressing the perception of official versus personality identity, and the respective values people attach to them, is essential in order to understand what personal information users are more and less willing, and perceive as more and less relevant to disclose in an eGovernment FIDMS.

Indeed, participants frequently expressed the perception of a ‘narrow’ identity in digital interactions, as they described themselves as engaging in selective disclosure of personal information all pertaining to a same overarching identity. In particular, participants disclosed information according to the digital contexts they were interacting in, the boundaries of which dictated the boundaries of the disclosed and ‘narrow’ identity facet. This relates to Goffman’s (1959) description of how people, when adapting to their social circumstances, carefully decide what personal information to share to ensure their desired outcome. Moreover, the findings relate to Altman’s (1975) theory of boundary regulation, whereby contextual boundaries regulate the information disclosed. Thus, the data supports established sociological theories of self-disclosure and extends the concepts to technological identity systems. A next step could be to identify any factors that distinguish self-disclosure in a digital versus physical and social context, to inform a *socio-technical* framework.

The disembodiment of the identification process characteristic of digital identity (Rahaman, 2012) led participants to attach specific properties to digital identity, dissociating it from physical identity. Notably, participants considered digital identification to be far less rigorous than physical identification and perceived loss of control of their personal information once shared digitally. Moreover, participants perceived the digitisation of their personal information to reduce them to an impersonal statistic in the overall user population. The hitherto technology-centred focus on identity systems (Lips et al., 2005; Rahaman & Sasse, 2011) may have contributed to this. These perceptions of disembodiment are important to address in FIDMS, to ensure that users feel they are citizens engaging with the government, rather than far removed pieces of data subject to the technological system.

5.1.2. Levels of Interaction: The Identity Ecosystem

This study unravelled the broader perceptions and relationships users have with digital identity, adhering to Rahaman & Sasse's (2011) proposal of exploring the *'lived experience'* of identity. Importantly, the findings are grounded in a user-centred perspective, examining digital identity not only as belonging in a technological vacuum, but identifying it as belonging to a layered identity ecosystem. Five levels of digital identity interaction emerged from the data: individual, technological, organisational, societal, and ethical – all influencing how participants use their personal information with eGovernment services. To achieve user-centred design in eGoverment FIDMS, these influences must be addressed in their implementation.

Trust forms a significant part of the technology-centred perspective on identity research. The present study went beyond the technology-centric view, identifying non-technological sources of trust, and trust as the essential basis for people's relationship to organisations and society as a whole. One source of trust was participants' previous experiences with sharing their personal information online: the majority of participants were comfortable with the security of the login process, having had no negative security experiences; whereas the few participants who either had experienced problems personally, or had friends with negative experiences, felt significantly less comfortable. This supports Bubas et al.'s (2008) argument that past experiences, and not just features of the interface itself, e.g. a padlock sign, contribute to higher levels of trust. Moreover, a salient finding was that participants distinguished between trust in the organisation's *intent* to protect, and trust in the organisation's *technological ability* to protect their users. Compared to non-government organisations, participants trusted government organisations more, as it was expected that government organisations would be held more accountable were personal information to go missing. This was due to their role as entitled necessities in people's lives, supporting the view of McKenzie et al. (2008) that government services are trusted more due to their societal responsibility to be transparent and inclusive. However, participants dissociated *perceived* security from *actual* security, stressing that even if they only perceived the identity system to be secure, it nevertheless increased its trustworthiness. This is previously discussed in literature (e.g. Rahaman, 2012). Crucially, this study found that the combination of perceived security and trust in the government organisation's integrity increased their overall level of trust.

Responsibility when sharing, storing, and collecting personal information was another salient concept transcending several layers of the identity ecosystem, in particular in the societal and ethical layers. Participants considered the use of their identifying information advantageous for national security and population survey purposes. As digital identity systems reduce the physical and temporal boundaries of individual-to-government interactions, both population protection and behaviour surveillance can be facilitated (Taylor et al., 2006; Bauer et al., 2005 in: FIDIS, 2005). Participants acknowledged this benefit; however, they stressed the importance of the government maintaining their responsibility to preserve individuals' rights not to be singled out for monitoring. Moreover, they questioned the actual benefit of enhancing national security, believing this would only further improve the technological sophistication of hackers and terrorists, which would require the government to increase their security further. However, participants agreed that government surveillance was for *"the greater good"* (P1) and would *"make society safer"* (P11), suggesting that they felt they were individually morally responsible to give up some personal information for the collective benefit. Indeed, Buckingham (2008) describes a facet of identity as the individual's belonging with a broader social group. The impact of culture in these values should be further explored, as culture-specificity of governments has been found to influence individuals' perceptions of IDMS (McKenzie et al., 2008). Non-UK participants in the present study did highlight some differences between the UK government and their home government: for example, P8 perceived the UK government exhibit more moral responsibility than the government in her native People's Republic of China. However, larger participant samples are needed for stronger conclusions.

According to Damiani et al. (2003), a key role of eGovernment IDMS is to facilitate trust relationships between individuals, organisations, and policy makers, i.e. the government. The present study has validated the intricate interplay between identity and these relationships. This study also suggests there is a need to clarify the moral responsibility of the individual versus the identity system versus the government in protecting personal information online, given the disparate views of the participants, and their consequent behaviours. For instance, as a minority of participant perceived personal information online to be exempt from the ethical norms of the offline world, the development of policies and guidelines for privacy protection is warranted.

5.1.3. eGovernment Identity in Everyday Life

It was found that interacting with eGovernment had a different, more compartmentalised role in participants' everyday life compared to other online activities. In particular, participants tended to interact with eGovernment with a concrete task in mind, and ended the interaction once the task was completed. This contrasts with the fluid, ill-defined, and longer-lasting browsing behaviour characteristic of social networking sites (Benevenuto, 2009). Furthermore, participants were frequently found to perform several tasks with separate, but often related, government services in a single session. This supports the view that the disembodiment of identification processes facilitates the integration of government-related activities (Marx, 2006): the absence of physical anchors brings users closer to the organisation (Damiani et al., 2003). Thus, it can be argued that digitising government services and personal information introduces seamlessness to the citizen-government interaction (Pollitt, 2003). Importantly, this seamlessness was disrupted when physical interaction was required, e.g. when login failed and participants needed to phone the service. This suggests that users compartmentalise their interactions as belonging to the digital environment only. Further study could address what cues might be necessary to facilitate the seamlessness between physical and digital government interaction.

Salient aspects of the role of eGovernment interactions were the sense of personal empowerment and control it provides participants. While it has been argued that the disembodiment of identification brings convenience for the authenticating organisation (Norlin & Durand, 2002; Taylor et al., 2006), this study also found it significantly empowering for the authenticated individual. Performing tasks with their digital identity was found to free participants from time constraints, physical anchors and locations, and also saved them money. Moreover, participants appreciated having access to and overview of the personal information stored with government services. This allowed them to complete tasks themselves, e.g. print out their medical prescriptions from their healthcare provider to pass on to Student Finance (P5). This strongly supports Mäkinen's (2006) idea of digital empowerment: eGovernment allows citizens to no longer be passive recipients engaging in a one-way interaction with government services, but rather active participants taking control of their lives in digital society. Crucially, further eGovernment development must uphold principles of *social inclusion* (McKenzie et al., 2008) and *universal access* (Lips & Pang, 2008) to ensure digital empowerment to all members of society, irrespective of technological proficiency.

Indeed, inadequate technical implementation of identity systems was detrimental for participants' experience of eGovernment in everyday life. The '*patchwork of identity one-offs'* (Cameron, 2005) was salient as participants had separate login details and procedures for each government service: password fatigue (Jøsang et al., 2007) was observed as participants either wrote passwords down or used the same passwords for several accounts, thus counteracting the intended security of maintaining separate login procedures (Adams & Sasse, 1999). Importantly, eGovernment services were not frequently used as a matter of routine, as social networks and media are: HMRC, for instance, is normally used once a year – and thus not recorded in any of the video diaries – and, as participants explained, would necessitate a password retrieval procedure every time HMRC is used. This automatic reliance on password retrieval is one of several reasons presently identified that necessitates design implications that take into consideration the broader, everyday relations between account logins and users' lives.

5.2. Design Implications for eGovernment FIDMS

To fulfil the aims of developing FIDMS for eGovernment facilitating trust relationships between all actors involved, enhancing security, and providing a seamless experience of a joined-up government for users, a user-centred approach must be taken. This study demonstrates that users not only interact with identity and government via technology, but also in the context of their everyday lives and relationships to organisations and society. Based on the findings from the present study, highlighted design implications are discussed that support and extend the guidelines outlined by Cameron (2005) and Dhamija and Dusseault (2008):

- *Ensure agendas of federation members are clear and justified*

  Participants were strongly against including third parties in the federation, expressing concerns that these might have their own commercial agendas. Members of the FIDMS should be clear in having the same non-commercial agendas as well as explicitly justify the collection and exchange of users' personal information.

- *Keep users informed without treating them as security experts*

  Participants desired to be asked for consent if SPs were to exchange their personal information amongst the federation or with third parties. However, participants felt uncomfortable being in control of the security of their accounts, due to their limited knowledge of technology. The FIDMS should therefore autonomously ensure sufficient security is maintained according to the requirements of the accounts without overwhelming users with decisions they are unqualified to take. Simultaneously, the system should keep users informed of what information is shared and not shared.

- *Facilitate completion of users' primary task*

  Participants' primary aim was to complete their concrete task efficiently and effectively. Moreover, during interaction, participants did not reflect over the interface, login procedure, or technology, but rather over acquiring the relevant information and completing their task. Design should minimise the interruption of the login procedure by keeping the login procedure brief and simple, to facilitate seamless task completion. Simultaneously, reassurance of security should be made explicit, albeit not require unnecessary action by the user.

- *Adhere to expectations and leverage established routines*

  Participants became confused and frustrated when redirected to websites other than that pertaining to their intended task. Moreover, login requirements outside the standard username/password procedure, particularly the need for physical artefacts such as library cards and Student Finance documents, was time-consuming, frustrating, and disrupted the flow of the interaction. The FIDMS should avoid introducing additional, less familiar, steps to the login process such as physical cards or tokens, or redirections to other websites. If physical authentication is required, this should be implemented once at initial registration, rather than constitute the routine of logging in.

- *Adhere to the dynamics of users' life situations*

  Changes in participants identifying information often failed to synchronise with the information stored in eGovernment user accounts, causing participants to forget how to login and have to access each account to change the same information. The FIDMS should therefore ensure that changes in users' digital identity are updated synchronously across all members of the federation. Moreover, participants use habits with different services depended on changes in their life situations, such as changing employment or commencing an academic year. The FIDMS should therefore not assume eGovernment use as a matter of routine, but be sensitive to the fact that users may in periods use services more or less frequently, or not at all for extensive periods of time.

- *Adhere to users' technology needs and use*

  Tasks with government services were often brief. Moreover, certain services were frequently used away from home, and as participants disliked the perceived privacy intrusion of performing government service tasks on shared or public computers, services were used on mobile devices. eGovernment design should therefore extend to mobile devices, e.g. by developing mobile applications of services that are frequently used on the move.

5.3. Limitations

There were some limitations of the present study that can be improved to enhance the generalisability of the conclusions.

Firstly, the recruitment procedure led to a suboptimal and restricted participant sample that was not representative of the general UK population and the variety of government services relevant for a FIDMS. Rather, the users were in a limited age group (in their 20s), all in – or recently at – university, all located in the Greater London area, and nearly all scoring highly on the personality trait of Openness to Experience. To investigate the behaviours and perceptions of the target population for eGovernment FIDMS in order to generate well-substantiated user requirements, a more varied sample must be selected. This includes users of all age groups above 18 years; of varied socioeconomic status, education levels, and occupational roles; and of varied geographical location. Presumably, this would ensure a significantly more representative distribution of government services and personality traits.

Secondly, due to the time constraints of the study, and to maintain participants' motivation, a two-week interval per participant was decided upon. This duration was neither sufficient to cover more long-term dynamic interaction patterns, behaviours, and influences, nor to cover infrequently used government services. To capture long-term behaviour, a video diary study would not be feasible given the amount of effort required. Hence, alternative research techniques should be employed for a more longitudinal study.

Thirdly, recording the video diary introduced an artificial element into participants' regular behaviour when interacting with government services, as revealed by the interview halfway through the two-week period. Participants said the recording slowed down their interaction and was slightly awkward to use initially as they were figuring out how best to position the camera. Apart from this, most participants said their behaviour was representative of how they would have interacted in the absence of the camera and felt that they successfully avoided purposely initiating an interaction due to their participation in the study. Some participants, however, experienced the setting as forced, in that they had to articulate thoughts they would not otherwise have. This may have biased their reflections in subsequent interviews.

Finally, the design implications are high-level and may be challenging to implement in design without more specific guidelines. Arguably, such specific guidelines cannot be developed until future research has established lower-level requirements, such as the best means of communicating security and which eGovernment services most warrant mobile applications.

5.4. Future Work

This qualitative study explored the as of yet ill-defined and insufficiently documented area of user interactions with digital identity and eGovernment in everyday life. The findings help to develop a framework from which more specific hypotheses can be tested in controlled studies, such as quantitative surveys and experimental laboratory studies.

Online surveys could collect large amounts of data on quantitative factors, such as which government services people use the most and at what time of year; which services people would wish to constitute a federation and which they would wish were excluded; and what personal information people perceive to be relevant and irrelevant to disclose. Moreover, collecting demographic information – such age, gender, personality traits, education levels, socioeconomic status and geographical location – from a large sample of users could identify correlates of eGovernment and digital identity behaviour and perceptions. Further to this, performing factor analysis on an extensive attitude questionnaire collecting self-reported behaviours and perceptions could identify salient and relevant factors. These factors could also contribute to data triangulation and theoretical refinement of the findings in the present study.

Experimental studies could manipulate controlled and independent variables identified as of interest in the present study, in order to investigate their effects on behaviour, perceptions, and interaction. An interesting variable would be the type of services used, to compare the experience of interacting with non-commercial government services versus commercial government services versus private services. Another relevant variable is the user's nationality: given the multicultural composition of the UK population, non-UK citizens will inevitably constitute the target user population of an eGovernment FIDMS. Given the finding that citizens of different countries have different levels of trust towards their governments, as well as the limited culture reflections observed in the present study, it would be highly interesting to explore the effects of cultural background on behaviours and perceptions of a UK FIDMS. These variables can e.g. be implemented in usability lab studies evaluating prototypes of an eGovernment FIDMS.

CHAPTER 6 **CONCLUSION**

This study investigated the behaviours and perceptions of eGovernment users in terms of the digital representation and disclosure of personal information; managing multiple eGovernment user accounts in everyday life; and FIDMS for eGovernment. Crucially, the study adopted a user-centred perspective of digital identity and eGovernment, aiming to explore the underlying human factors pertaining to individuals' interactions. It found that users perceive digital identity in eGovernment as a disembodied, impersonal, and multifaceted construct that is constrained by the contexts in which each facet is used. Their perceptions were mediated by how they perceived themselves, the interface and the overarching service providing organisation, as well as the societal and ethical implications of disclosing personal information. Moreover, the study identified factors beyond the mere relationship between the user and the eGovernment website that influenced the interaction. These include the dynamics of users' everyday lives in terms of needing to use certain services more and less in periods of their lives; and that technology is increasingly used with mobile devices while on the move. Finally, the study identified salient problems with managing multiple separate accounts, and participants' perceptions of the merits and limitations of using federated accounts for eGovernment.

Of particular note, this study is the first to research the *reality* of users' eGovernment behaviour in everyday life, using an innovative research technique, namely video diary studies. This technique successfully captured user experiences and behaviours more holistically as it verified and extended interview data. This revealed factors that the researcher and participants could have neglected to attend to, and factors difficult for participants to articulate overtly in interviews, such as interrupted interactions. Moreover, participant-driven data collection advantageously reduces the time and effort necessary to be invested by the researcher. Further to this, the interviews reached a point of information saturation, strengthening the completeness of the data set.

The take-home point from this study in terms of the development of FIDMS for eGovernment, is that designers must look beyond the technology-centred aspects of identity management. Instead, they should consider how users experience the sharing of their personal information, in particular what facets of identifying information users are more and less comfortable with sharing. Designers should also consider what features of the organisations they interact with facilitate or inhibit their interactions; and how such interactions fit into the overall contexts of users daily lives. Only then can the lived experience of identity be captured and supported, towards truly user-centred identity management.

REFERENCES

Adams, A. & Sasse, M.A. (1999). Users are not the enemy: Why users compromise security mechanisms and how to take remedial measures. *Communiations of the ACM, 42,* 40-46.

Adams, A., Lunt, P., & Cairns, P. (2008). A qualitative approach to HCI research. In P. Cairns & A. Cox (Eds.), *Research Methods for Human-Computer Interaction* (pp. 138-157). Cambridge, UK: Cambridge University Press.

Alpár, G., Hoepman, J.-H., & Siljee, J. (2011). The identity crisis: Security, privacy and usability issues in identity management. *Management,* 1-15.

Altman, I. (1975). *The Environment and Social Behavior.* Monterey, CA: Brooks/Cole.

Arora, S. (2008). National e-ID card schemes: a European overview. *Information Security Technical Report, 13,* 46-53.

Baldoni, R. (2012). Federated identity management in e-government: the case of Italy. *Electronic Government, 9,* 64-84.

Barsalou, L.W. (1988). The content and organization of autobiographical memories. In U.N.E. Winograd (Ed.) *Remembering Reconsidered: Ecological and Traditional Approaches to the Study of Memory* (pp. 193-243). Cambridge University Press.

BBC (2010). Identity card scheme will be axed 'within 100 days'. *BBC News.* Retrieved from news.bbc.co.uk/1/hi/uk_politics/8707355.stm on 27 March 2012.

Benevenuto, F. (2009). Characterizing user behavior in online social networks categories and subject descriptors. *Transition, 20,* 49-62.

Berg, B.L. (2001). *Qualitative Research Methods for the Social Sciences.* Boston"

Allyn and Bacon.

Beyer, H. & Holtzblatt, K. (1997). *Contextual Design: Defining Customer-Centered Systems.* San Francisco: Morgan Kaufmann Publishers Inc.

Bonneau, J. & Preibusch, S. (2010). The password thicket: Technical and market failures in human authentication on the web. *Proceedings of WEIS 2010: The 9th Workshop on the Economics of Information Security.* Boston, MA, 25 June 2010.

Bubas, G. Orehovacki, T., & Konecki, M. (2008). Factors and predictors of online security and privacy behavior. *Journal of Information and Organizational Sciences, 32,* 79-98.

Buckingham, D. (2008). Introducing identity. In D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (pp. 1-24). Cambridge, MA: The MIT Press.

The Cambridge Dictionary of Philosophy (2nd Ed.) (2005). Cambridge University Press.

Cameron, K. (2005). *The Laws of Identity.* Retrieved from http://www.identityblog.com/stories/2004/12/09/thelaws.html on 5 February 2012.

Camp, L.J. (2003). Design for trust. In R. Falcone (Ed.) *Trust, Reputation and Security: Theories and Practice.* Berlin: Springer-Verlang.

Camp, L.J. (2004a). Digital identity. *Technology and Society Magazine, IEEE, 23,* 34-41.

Camp L.J. (2004b). Identity in Digital Government. *papers.ssrn.com.* Cambridge, MA: Harvard University.

Camp, L. J. (2007). *Economics of Identity Theft: Avoidance, Causes, and Possible Cures.* London: Springer.

Carter, S. & Mankoff, J. (2005). When participants do the capturing: the role of media in diary studies. In *Proceedings of the SIGCHI Conference of Human Factors in Computing Systems* (pp. 899-908). New York: ACM.

Chadwick, D.W. (2008). Federated identity management. *FOSAD 2008,* 96-120.

Clarke, R. (1997). *Introduction to Dataveillance and Information Privacy, and definition of Terms.* Retrieved from www.cse.unsw.edu.au/~se4921/PDF/Other/roger-clarke-intro.pdf on 13 March 2012.

ComputerWorld UK (2012). Data privacy concerns put citizens off online contact with government. *ComputerWorld UK.* Retrieved from www.computerworlduk.com/news/public-sector/3355911/data-privacy-concerns-put-citizens-off-online-contact-with-government/ on 10 May 2012.

Costa, P.T. & McCrae, R.R. (1992). Reply to Eysenck. *Personality and Individual Differences, 13*, 861-865.

Cottrell, R. (2010). *User-Centred Identity Management: Evaluating the Role of the Browser.* Retrieved from www.ucl.ac.uk/uclic/taught_courses/distinction on 5 February 2012.

Cranor, L.F. & Reagle, J. (1998). Designing a social protocol: Lessons learned from the Platform for Privacy Preferences Project. *Proceedings of the Telecommunications Policy Research Conference TPRC97,* 1-15.

Crompton, M. (2002). *Under the Gaze, Privacy Identity and New Technology*. Paper presented at the Australian IT Security Forum, 30 March 2004.

Damiani, E., di Vimercati, S.D.C., & Samarati, P. (2003). *IEEE Internet Computing.* IEEE. Retrived from ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1250581&isnumber=27995&u

rl=http%3A%2F%2Fieeexplore.ieee.org%2FstampPDF%2FgetPDF.jsp%3Ftp%3D%26arnumber%3D1250581%26isnumber%3D27995 on 16 February 2012.

Dhamija, R. & Dusseault, L. (2008). The seven flaws of identity management: usability and security challenges. *IEEE Security & Privacy, 6,* 24-29.

Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590).

Durand, A. (2003). *Updating the Tiers of Identity.* Retrieved from www.andredurand.com/?p=147 on 25 February 2012.

eDT (2005). *UK Government Gatewat – EP02 Gateway Business Briefing.* London: eGovernment Unit.

Ellison, C.M. (2002). Improvements on conventional PKI wisdom. *1st Annual PKI Research Workshop April 2002,* Dartmouth, NH.

Flórencio, D. & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web, May 8-12, 2007*. Banff, Alberta, Canada.

Future of IDentity in the Information Society Project (FIDIS) (2005). WP2, D2.1. *Inventory of Topics and Clusters,* 21 September 2005.

Gilbert, D., Kerr, I.R., & McGill, J. (2006). The medium and the message: Personal Privacy and the forced marriage of police and telecommunications providers. *Criminal Law Quarterly 51,* 469.

Goffman, E. (1959) *The Presentation of Self in Everyday Life*. New York: Doubleday.

Google Inc. (2008). *Google's Internet Identity Research. Usability Research on Federated Login.* Retrieved from sites.google.com/site/oauthgoog/UXFedLogin on 16 February 2012.

Gosling, S.D., Rentfrow, P.J., & Swann Jr., W.B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in Personality, 37,* 504-528.

Grawemeyer, B. & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23,* 256-267.

Greenwood, D. (2007). The context for Identity Management Architectures and Trust Models. *Proceedings of the OECD Workshop on Digital Identity Management,* Trondheim 2007.

Jeong, Chun Hai (2007). *Fundamental of Development Administration.* Selangor: Scholar Press.

Jones, M., Wilson, M. L., Craggs, D., Robinson, S., Jones, M., & Brimble, K. (2011). Pico-ing into the future of mobile projection and contexts. *Personal and Ubiquitous Computing*, *16*, 39-52.

Jøsang, A. & Pope, S. (2005). User-centric identity management. *AusCERT Conference 2005*. Retrieved from http://folk.uio.no/josang/papers/JP2005-AusCERT.pdf on 5 February 2012.

Jøsang, A., Zomai, M. A., & Suriadi, S. (2007). Usability and privacy in identity management architectures. *Fifth Australasian symposium on ACSW frontiers* (pp. 143–152). Darlinghurst, Australia: Australian Computer Society.

Kamsin, A., Blandford, A., & Cox, A. (2012). Personal task management: my tools fall apart when I'm very busy! In *Proceedings of the 2012 ACM Annual Conference Extended Abstracts on Human Factors in Computing Systems Extended Abstracts* (pp. 1369-1374). New York: ACM.

Kakali, P. (2010). *Towards OpenID Interoperability.* (Unpublished MSc dissertation).]University College London, London UK.

Lips, A.M.B. & Pang, C. (2008). *Identity management in information age* *government: exploring concepts, definitions, approaches, and solutions.* Victoria University of Wellington. Retrieved from http://www.egov.vic.gov.au/focus-on-countries/pacific-region/new-zealand/trends-and-issues-new-zealand/identity-management-new-zealand/identity-management-in-information-age-government-exploring-concents-definitions-approaches-and-solutions-in-pdf-format-558kb.html on 10 May 2012.

Lips, A.M.B., Taylor, J., Organ, J. (2005). Electronic government: towards new forms of authentication, citizenship and governance. *Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities.* Oxford, UK: Oxford Internet Business School.

Lyon, D. (2007). National ID cards: crime-control, citizenship and social sorting. *Policing, 1,* 111-118.

Lyon, D. (2009). *Identifying Citizens: ID Cards as Surveillance.* Cambridge, UK: Polity.

Mäkinen, M. (2006). Digital empowerment as a process for enhancing citizens' participation. *E-Learning and Digital Media, 3,* 381-395.

Maler, E.E. & Reed, D. (2008). The venn of identity: options and issues in federated identity management. *IEEE Security & Privacy, 6,* 16-23.

Marx, G.T. (2006). Varieties of Personal Information as Influences on Attitudes Toward Surveillance. In K. Haggerty & R. Ericson (Eds.), *The New Politics of Surveillance and Visibility*, Toronto: University of Toronto Press.

McKenzie, R., Crompton, M., & Wallis, C. (2008). Use cases for identity management in E-Government. *IEEE Security & Privacy, 6,* 51.57.

Nentwich, F., Kirda, E., & Kruegel, C. (2006). Practical Security Aspects of Digital

Signature Systems. *Secure Systems Lab, Technical University of Vienna.* Retrieved from www.iseclab.org/papers/citizen_technical.pdf on 15 March 2012.

Norlin, E. & Durand, A. (2002). *Towards Federated Identity Management.* Retrieved from www.andredurand.com/?p=134 on 17 March 2012.

Office of the eEnvoy (2002). *Registration and Authentication – eGovernment Strategy Framework Policy and Guidelines – Version 3.0*. London: Office of the eEnvoy.

Ones, D.S., Viswesvaran, C., & Schmidt, F.L. (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology, 78,* 679-703.

Pfitzmann, A. & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *Identity*. Retrieved from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml on 29 May 2012.

Pfitzmann, K., Hansen, M., Liesebach, K., Pfitzmann, A., & Steinbrecher, S. (2006). What user-controlled identity management should learn from communities. *Information Security Technical Report*, *11*(3), 119-128.

Pollitt, C. (2003). Joined-up government: A Survey. *Political Studies Review, 1,* 34-49.

Popper, K.R. (1959). *The Logic of Scientific Discovery.* London: Huthinson Education.

Rahaman, A. & Sasse, A. (2010). A framework for the lived experience of identity: from rhetoric to reality. *Identity in the Information Society, 3,* 605-638.

Rahaman, A. (2012). *A Human-Centred Approach to Identity Management Systems*

(Unpublished doctoral dissertation). University College London, London, UK.

Sasse, M.A. (1997). *Eliciting and Describing Users' Models of Computer Systems.* University of Birmingham.

Sokolov, D. (2006b, February 7). Österreichs signaturanbieter A-Trust sucht den weg aus der krise. *HeiseOnline*. Retrieved from www.heise.de/newsticker/Oesterreichs-Signaturanbieter-A-Trust-suchtden-Weg-aus-der-Krise--/meldung/69316 on 15 March 2012. (Translated by Google Translate).

Strauss, A. & Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* New York: Sage.

Taylor, J., Lips, A.M.B, & Organ, J. (2006). The Citizen, the State and the ID Nexus: Attention to Information, Societal Shaping and Modes of Citizen Sorting. *Information, Communication & Society 10th Anniversary International Symposium,* University of York, 20-22 September 2006.

The Telegraph (2011). Coalition builds new national identity system. *The Telegraph.* Retrieved from http://www.telegraph.co.uk/technology/news/8526946/Coalition-builds-new-national-identity-system.html on 25 May 2012.

Wharburton, S. (2010). *Identity Matters.* London: King's College London.

White, P. (2008). *Managing Enterprise Complexity: The Use of Identity Management Architecture to Control Enterprise Resources.* Charles Sturt University.

Williams, S., Fleming, S., Lundqvist, K., & Parslow, P. (2010). Understanding your digital identity. *Learning Exchange, 1,* 1-5.

Windley, P. J. (2005). *Digital identity*. Sebastopol, California: O'Reilly.

Wilton, R. (2005). Positioning Federated Identity for the UK Government. *Sun*

Microsystems Ltd. Retrieved from www.projectliberty.org/liberty/resource_center/papers/member_papers/positioning_federated_identity_for_the_uk_government/index.html?noframe on 24 March 2012.

Yahoo! Inc. (2008). *OpenID: One Key, Many Doors – OpenID User Experience Research.* Retrieved from developer.yahoo.com/openid/openid-research-jul08.pdf on 16 February 2012.

APPENDIX A. RECRUITMENT QUESTIONNAIRE

Hello,

Thank you very much for taking the time to complete this survey.

This survey is part of a research project at UCL Interaction Centre and will only take approximately 5 minutes of your time. Your identity will be kept strictly confidential and not disclosed in any way. Only if you sign an informed consent form for the video diary study will your responses to the questions be reported or published in any way. If reported/published, your responses will not be linkable to you, maintaining your anonymity.

If you have any questions about the survey or the study overall, please contact me at s.zhuang@ucl.ac.uk.
There are 16 questions in this survey

Demographic Information

1 [1]Name *

Please write your answer here:

2 [2]Email *

Please write your answer here:

3 [3]Please indicate your age *

Please choose **only one** of the following:

- ○Under 18
- ○18-24
- ○25-34
- ○35-54
- ○55+

4 [4]Please indicate your gender *

Please choose **only one** of the following:

- ○Female
- ○Male

5 [5]What is the highest level of education that you have completed?

Please choose **only one** of the following:

- ○GCSE or less
- ○Completed A levels or equivalent
- ○Some university, no degree
- ○Associate/foundation degree or equivalent
- ○Bachelor's degree
- ○Postgraduate degree

6 [6]Please indicate your area of employment

Please choose **only one** of the following:

- ○Accounting / Finance / Banking
- ○Administration / Clerical / Reception
- ○Advertisement / PR
- ○Architecture / Design

- ○Arts/Leisure / Entertainment
- ○Beauty / Fashion
- ○Buying / Purchasing
- ○Construction
- ○Consulting
- ○Customer Service
- ○Distribution
- ○Education
- ○Health Care (Physical & Mental)
- ○Human resources management
- ○Management (Senior / Corporate)
- ○News / Information
- ○Operations / Logistics
- ○Planning (Meeting, Events, etc.)
- ○Production
- ○Real Estate
- ○Research
- ○Restaurant / Food service
- ○Sales / Marketing
- ○Science / Technology / Programming
- ○Social service
- ○Student
- ○Other
- ○N/A - Unemployed / Retired / Homemaker

Use of Online Public Services

7 [7]Please list the public services that you currently have a registered user account for. Below are some examples. Please add any services that are not included. *

Please choose **all** that apply:

- □Your public university user account(s)
- □The NHS: nhs.uk
- □Jobcentre Plus: jobseekers.direct.gov.uk
- □Student Finance: studentfinance.direct.gov.uk
- □Barclays Cycle Hire: web.barclayscyclehire.tfl.gov.uk
- □Congestion Charging: congestioncharging.tfl.gov.uk
- □Oyster Online: oyster.tfl.gov.uk
- □Low Emission Zone: lowemissionzone.tfl.gov.uk
- □East Coast: eastcoast.co.uk
- □Royal Mail: royalmail.com/personal
- □Carbon Calculator: carboncalculator.direct.gov.uk
- □Home Office UK Border Agency: homeoffice.gov.uk
- □Government Gateway (for e.g. DVLA, DWP): gateway.gov.uk

- □HM Revenue & Customs (for e.g. Self Assessment, Tax Return, Pension): directgov-online.hmrc.gov.uk
- □Your local authorities (for e.g. Council Tax, Parking, Library): e.g. london.gov.uk, cityoflondon.gov.uk, camden.gov.uk, rbkc.gov.uk, islington.gov.uk, etc.
- □Research/academia-related services: e.g. wellcome.ac.uk, nihr.ac.uk
- □Other:

8 [8]Please list the 3-5 services that you use the most *

Please write your answer here:

9 [9]For how long have you used your MOST recently registered account? *

Please choose **only one** of the following:

- ○Less than 1 month
- ○1-3 months
- ○4-6 months
- ○More than 6 months

10 [10]For how long have you used your LEAST recently registered account? *

Please choose **only one** of the following:

- ○Less than 1 month
- ○1-3 months
- ○4-6 months
- ○More than 6 months

11 [11]In an average week, how many different services will you use? *

Please choose **only one** of the following:

- ○None
- ○1 service per week
- ○2-3 services per week
- ○4-6 services per week
- ○More than 6 services per week

12 [12]In an average week, how many times do you use any of these services? Please add up the total number of times across all the services you use *

Please choose **only one** of the following:

- ○Never
- ○1-2 times per week
- ○3-4 times per week
- ○5-6 times per week
- ○More than 6 times per week

13 [13]In general, how do you feel about having to manage multiple user accounts online? *

Please write your answer here:

14 [14]Have you ever used federated login, i.e. logged in via one service once, and then had access to several other services?

Some examples include:

- **Login via Facebook/Twitter**
- **OpenID**
- **Single Sign-On**
- **Athens/Shibboleth**
- **Microsoft Account/Windows Live ID**
- **Google Mail**

Please choose **only one** of the following:

- ○Yes
- ○No
- ○Not sure

15 [15]If yes, do you have any thoughts on using systems like these?

Please write your answer here:

Personality Statements

Here are a number of personality traits that may or may not apply to you. Please indicate for each statement the extent to which you agree or disagree with that statement. You should rate the extent to which the pair of traits applies to you, even if one characteristic applies more strongly than the other.

16 [16]I see myself as... *

Please choose the appropriate response for each item:

	Strongly disagree	Moderately disagree	Slightly disagree	Neutral	Slightly agree	Moderately agree	Strongly agree
...extraverted, enthusiastic	○	○	○	○	○	○	○
...critical, quarrelsome	○	○	○	○	○	○	○
...dependable, self-disciplined	○	○	○	○	○	○	○
...anxious, easily upset	○	○	○	○	○	○	○
...open to new experiences, complex	○	○	○	○	○	○	○
...reserved, quiet	○	○	○	○	○	○	○
...sympathetic, warm	○	○	○	○	○	○	○
...disorganised, careless	○	○	○	○	○	○	○
...calm, emotionally stable	○	○	○	○	○	○	○
...conventional, uncreative	○	○	○	○	○	○	

Thank you for taking part in this survey. I will notify you if you are eligible for the video diary study.
01.01.1970 – 01:00

Submit your survey.
Thank you for completing this survey.

APPENDIX B. INFORMED CONSENT FORM

Informed Consent Form for Participants in Research Studies

Title of Project:	'Me, Myself, & I': Conceptualising Identity in Federated Identity Management for E-Government Services

This study has been approved by the UCL Research Ethics Committee as Project ID Number: MSc/1112/006

Participant's Statement

I ………………………………………….....................................

agree that I have

- read the information sheet and/or the project has been explained to me orally;
- had the opportunity to ask questions and discuss the study;
- received satisfactory answers to all my questions or have been advised of an individual to contact for answers to pertinent questions about the research and my rights as a participant and whom to contact in the event of a research-related injury;
- understood that my participation will be video and audio recorded;

I understand that I am free to withdraw from the study without penalty if I so wish, and I consent to the processing of my personal information for the purposes of this study only and that it will not be used for any other purpose. I understand that such information will be treated as strictly confidential and handled in accordance with the provisions of the Data Protection Act 1998.

Signed: Date:

Investigator's Statement

I, Susan Zhuang

confirm that I have carefully explained the purpose of the study to the participant and outlined any reasonably foreseeable risks or benefits.

Signed: Date:

APPENDIX C. INFORMATION SHEET

Information Sheet for Participants in Research Studies

You will be given a copy of this information sheet.

Title of Project: ‘Me, Myself, & I’: Conceptualising Identity in Federated Identity Management for E-Government Services

This study has been approved by the UCL Research Ethics Committee as Project ID Number: MSc/1112/006

Name, Address and Contact Details of Investigators:

Susan Zhuang
15 Clarence Gardens
London NW13LH
07543100141

We would like to invite you to participate in this research project. You should only participate if you want to; choosing not to take part will not disadvantage you in any way. Before you decide whether you want to take part, please read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or you would like more information.

The purpose of this research is to explore people’s use of multiple user accounts for public services online, e.g. for healthcare or taxation services, and people’s experience of digital identity. You will be asked to video record your use of such online services for a 2-week period, including when, where, and why you use a specific service at a particular time, and your thoughts surrounding the use of the service and the login procedure. You are free to disclose as much information as you wish in your recordings, but for the benefit of this research, you are encouraged to record in as much detail as possible.

Furthermore, you will be interviewed on 2 occasions: once at the beginning of the 2 weeks, and once at the end of the 2 weeks. These interviews will be audio recorded.

You will be reimbursed with a £50 Amazon voucher for your participation.

It is up to you to decide whether or not to take part. If you choose not to participate, you will not incur any penalties or lose any benefits to which you might have been entitled. However, if you do decide to take part, you will be given this information sheet to keep and asked to sign a consent form. Even after agreeing to take part, you can still withdraw at any time and without giving a reason.

All data will be collected and stored in accordance with the Data Protection Act 1998.

APPENDIX D. BRIEFING SCRIPT

Thanks a lot for helping out with my project. I'm investigating how people use public sector services online, in particular how they manage different user accounts for the different services, and how they relate to their digital or online identities.

This study will run across 2 weeks. Over the 2 weeks, you will keep a video diary, recording your experience with using public sector or government-related services online. Additionally, I'm interested in your behaviour with any accounts you have related to your university Intranet and research databases and research tools.

I'd like you to report the whole experience from when you approach your computer to perform a task with the government service, to after you've completed any task you may have on your account. I'd also like you to report any notable issues or incidents, like frustrations, problems, surprises, and so on. I'll give you an instructions sheet with more detailed information that you can refer to.

You're encouraged to be as detailed and thorough in your video recordings as possible for the benefit of my research, but it is up to you if there are elements you do not wish to disclose. I would like you to make video diary entries every time you use public services online to the extent possible, i.e. even when you're not at home, although I understand that this may sometimes not be possible. It's up to you how you wish to record your entries, whether you want to record yourself, your screen, or nothing at all. Also, before you submit the recordings to me, you're free to add, remove and edit the recordings as you wish.

I’ll remind you via email once in a while to remember to make the video diary entries, to collect your recordings, and to do a quick check up interview. You will meet me to be interviewed on 2 occasions. The first interview will be now, the second will at the end of the 2-week period. Before the last interview, I’d like you to have reviewed and submitted all your recordings to me.

The project has UCL ethics approval and is covered by the Data Protection Act, which means your identity will not be disclosed in any way and you will be kept completely anonymous in my final report. Also, your recordings will be deleted as soon as I’ve transcribed them into text. If you still agree to take part, please have a read through this information sheet and sign the informed consent form. Feel free to ask questions at any time.

APPENDIX E. INTERVIEW QUESTIONS

User Accounts, Password Management, and Personal Information

1. How many user accounts and passwords do you estimate that you have online in total?
2. How many of these are for public or government services in particular? Could you list those you use the most and describe the sorts of things you would use them for?
3. Do you ever experience frustrations when you've used government services online? Could you describe these?
4. How do you manage the usernames and passwords for the different services you're registered to?
5. Do you use the same email address for registering different accounts? Do you have any shared accounts?
6. When registering a new account, how much information do you give them? Does this differ across services? How do you feel about linking a profile picture with your account?
7. Do you ever give false information? Why/why not?
8. Do you think the Internet is fair game in terms of personal information or do you think there should be rules of conduct in terms of privacy online as it is in the physical world?
9. How does the process of logging into your account affect the overall task you are trying to accomplish?

eGovernment

10. Could you describe some of the things you like and dislike about using government services online?
11. Could you talk a little bit about what makes you decide to register to use a government service online; and what makes you decide to use that service at any given time?
12. How much do you trust government services online? What makes you trust or not trust them? Do you trust the UK government in handling your data?
13. How secure do you think it is using these services? What makes you think they are secure or not secure?
14. How would you compare the experience of using government services in the real world and online?
15. What are your thoughts on the government increasingly digitising their services?

Digital Identity

16. What do you think digital/online identity is?
17. How would you define your own digital/online identity? How does this definition relate to your real-world identity?
18. How would you compare the notion of physical identity vs. digital identity? In particular the aspect of verifying your own identity? How would you compare this for public services or government-related services in particular?
19. What aspects of your identity would you say you value the most and what information do you think is the most important for someone to identify you?
20. How much in control of your digital identities do you feel you are? Or how much ownership of your accounts do you feel you have?

21. What image of you do you think the government service providers can create of you from the personal information you provide?

Federated Identity Management

22. Imagine that the UK government implements a federated login system where you can login via one identity provider (e.g. the Royal Mail) which stores your login details, in order to access your user accounts with other service providers (e.g. the NHS, TfL, etc.). What are your thoughts on this?
23. How would you feel about the government collaborating with non-government services? For example, you would login via your account with Facebook, VISA, PayPal, Experian, etc. in order to access your accounts with government services.

Online Presence and Tracking

24. To what extent are you concerned that other agents but yourself, such as the service provider, know what you do with your accounts?
25. If you think the service providers track your account use, what do you think they would use it for and what are your thoughts on it?
26. Are there accounts you would have less reservations for in terms of being tracked than others?
27. Do you change your behaviour with an account in any way depending on what you use it for and what information it contains?
28. What are your thoughts about your online presence as a consequence of what you have do with your different accounts?

APPENDIX F. VIDEO DIARY INSTRUCTIONS

Instructions for making video diary entries

1. Please consider the following situations that you might experience while using government-related services online

- You form the intention of using one or several government-related services online
- You start preparing to login to your user account for a government-related service
- You retrieve your login details
- You struggle to remember your login details
- You are interrupted while using a public service
- You begin using the government-related service but then decide not to
- You experience other situations making it difficult for you, or preventing you from, using the government-related service
- You do not really know how to go about doing what you intend to do on the government-related service
- You provide the system with your personal government-related
- You realise that you need to use another public service as well
- You try to reflect on how you manage your different user accounts

2. If you experience any of the above situations, or similar situations, throughout the period of the study, please tell me more about them based on the following prompts:

1. **What service am I going to use and why? Why did I decide to use this service now?**
2. **Where and when am I using this service? Are there any other people around while I'm using this service?**
3. **How do I access the website? Is it difficult or easy?**
4. **How do I remember my username and password?**
5. **As I'm using the service, what am I doing, thinking and feeling? Do I trust the service?**
6. **What features of the service make me feel [frustrated, satisfied, secure, suspicious…]?**
7. **As I've finished using the service, what am I doing, thinking, and feeling?**

3. Please use the Flip Mino video recorder provided to record the information

    1. To start recording, please press the red button in the middle of the device. The red light at the back of the device will be on when recording is in progress. To stop recording, please press the red button again.
    2. If the device's internal flash memory is running out of space, please inform the researcher so she can replace it immediately. The flash memory can hold approximately 1 hour's video.
    3. If the battery life is running low, please replace them with the two AA batteries provided.
    4. It is advisable to immediately record the information at the moment when you experience the situation. Therefore, I would encourage you to bring the device with you at all times.

You will be contacted by the researcher from time to time to check whether or not you need further assistance or information about the study. You will also be asked on occasion to submit via email the recordings you have made so far. Prior to submission, you are allowed to view, add, remove, and edit entries as you wish.

Thank you very much for your participation!

APPENDIX G. EXAMPLES OF TRANSCRIPTS

P13_interview

Okay. So what's-, what's your opinion of the government increasingly digitising services?

[pauses]

Do you feel like society's online then, there's no distinct boundary between society online and society in the real world, or do you-

Uh. Basically, yeah [laughs], or… Um. [pauses] Maybe they want everything increasingly digitised in order to monitor people better. It's always supposed to be for our protection anyway. So for terrorists messing around, they can track them down if everything's-, if their details are already on some kind of-, online system. But again it does feel like, uh, so-, it's a so-called Big Brother state where everything has to be online, everything has to be controlled. Maybe I'm a bit uncomfortable with that, but it's gonna happen anyway, there's no way of fighting it. It's just the way it is.

P12_video

So I just got there through Google, so I'm on the Camden…um, library's home page now. So…I'm just gonna select West Hampstead Library, 'cause that's my local library, I'm at home at the moment in London. Um. [displays West Hampstead Library page] I've never-, I've only ever used this site to sign up, but it's raining outside, and I can't really bother to go down and renew my books, so. Oh, it says here I can renew my library items, brilliant [selects ’How do I renew my library loans?’], so I’m gonna click that. Um. I’m not really very-, um, ‘cause I’ve only been here a second time, I’m not very familiar with it, so it might take me a little while to get in [displays login page]. So…okay, my customer ID and my PIN I need, and I need my-, customer ID is the barcode for my library card, so. Right. [looks for library card] I’ve got my library card here, woo [shows library card], and, so, my, oh, it’s a very, very, very long number, I mean, look at that [shows barcode number], it’s a *long* number that I have to put in there. [reads out 14 digits] okay. Luckily I’ve got good eyesight, ‘cause otherwise I don’t know how someone could read that, it’s really tiny letters [laughs]. Um. My PIN…okay. I don’t know what my PIN is [laughs]. Um. It would help if I had a little tip, ‘cause I’ve got a good little tip here saying, ‘your customer ID is the barcode from your library card’, but for the PIN, it doesn’t really have anything. But I’m just gonna try my…my date of birth and stuff [displays Accept Cookies window] Ah! That’s good, it worked first time [laughs].