End report IMPRINTS:

What do users want from their future means of Identity Management?

Liesbet van Zoonen for Imprints

September 2014
IMPRINTS project team

Pam Briggs
Lilia Gomez Flores
Dougie Kinnear
Aletta Norval
Elpida Prasopoulou
Lisa Thomas
Georgina Turner
Sharon Walker
Sandra Wilson
Liesbet van Zoonen
Executive Summary

1 Introduction

2 Existing Research
   2.1 Concerns and attitudes towards (online) privacy
      2.1.1 What do people consider ‘personal data’?
      2.1.2 Who can be trusted with your personal data?
      2.1.3 What is the context of the personal data exchange?
      2.1.4 How is personal data collected and is it appropriate to its purpose?
      2.1.5 Do different people have different privacy concerns?
      2.1.6 Conclusion
   2.2 Accepting new technologies of IM
      2.2.1 Biometrics
      2.2.2 Smart cards
      2.2.3 Alternatives to passwords
      2.2.4 Smart wearables
      2.2.5 Conclusion

3 Questions & Design

4 Current practices of Identity Management by the UK public
   4.1 Usage
   4.2 Problems
   4.3 Pleasures
   4.4 Discussion

5 Future forms of Identity Management
   5.1 Desires and taboos
   5.2 Differences between users
   5.3 Differences between context of use
   5.4 Discussion

6 Future functions of Identity Management
   6.1 Desires and taboos
   6.2 Differences between users
   6.3 Differences between context of use
   6.4 Discussion

7 Future governance of Identity Management
   7.1 Desires and taboos
   7.2 Differences between groups
   7.3 Differences between context of use

8 Discussion
9 Recommendation
  9.1 Recommendations for designing, developing and implementing new IM systems 32
  9.2 Recommendations for regulation and governance of IM schemes 34
  9.3 Recommendations for further research 34

10 References 36

Appendix 1: Sources for more methodological detail
Appendix 2: Research design
Appendix 3: Impact
1. ‘Identity management’ (further: IM) has been identified as one of the key challenges of the future by governmental, corporate and civic stakeholders, yet at present it is not a key concern of the public at large.

2. The way the public at large manage their identities can be characterised by a ‘privacy paradox’, meaning that people eagerly share their personal data in one situation, while refusing them in other situations. For the future and inevitable expansion of identity management, it is crucial to understand this privacy paradox.

3. Existing research about the public’s acceptance of new forms of identity management has focused on people’s concerns about privacy on the one hand, and their attitudes towards new technologies on the other.

4. With respect to privacy, existing research makes clear that:
   a. people consider financial, medical and civic data as their most personal and sensitive information; increasingly people consider their social media data as very private;
   b. health organisations and banks come out as most trusted organisations, internet and phone companies, as well as search engines and social network sites as least trusted and even as a threat to privacy;
   c. privacy concerns are dependent on place, time, context of using personal data, and on the way these data are collected;
   d. there is no clear picture as to if and how privacy concerns differ along socio-demographic and cultural lines.

5. With respect to new IM technologies, the existing research has focused on:
   a. the acceptance of biometrics and smart cards in particular;
   b. the relative advantages that people perceive in these technologies, especially with respect to ease of use and efficiency;
   c. a limited model of technology use which has little attention for contextual and individual differences, nor for the (cultural) meanings that people ascribe to new IM technologies.

6. Our research asks questions about people’s current usage and appreciation of IM technologies, and about their desires and taboos regarding future forms, functions and governance of new IM technologies.

7. We have conducted 8 different empirical studies through different kinds of triangulation to produce research outcomes about taboos and desires for IM in more than 200 different combinations of type of IM technology, user and contexts.

8. In addition to this diversity we also find general tendencies that hold across
current usage, and future forms, functions and governance of IM.

9. Current practices of IM:
   a. Our inventory of the different means of identification and authentication that people currently have at their disposal, and the problems and pleasures they experience with them, suggest strongly that for the ordinary citizen or consumer IM is not much of an issue yet, neither in positive nor in negative terms.
   b. The possessions of means of IM is clearly socially stratified with vulnerable groups having less means of IM and experiencing more problems.
   c. While people regularly expressed a concern about cybercrime and a desire for the government and the police to do more against it, this did not result in highly reflective and secure procedures for themselves.
   d. We thus see the privacy paradox reflected in current usage of IM.

10. With regards to the future forms of IM that are being imagined or developed, we found that:
    a. People experience little need for them or benefit of them;
    b. The desire to use these new forms of IM depends on a number of basic factors regarding safety and security that need to be realised before considering them;
    c. The desire to use these new forms of IM, in addition, depends on whether people are already familiar with them, whether they can be personalised, whether people find them to be in good taste or ‘cool’;
    d. Groups of people tend to differ in terms of their degree of reluctance towards new forms of IM, but we found no groups who could be identified as likely early adopters of new forms of IM;
    e. People’s perceptions of these new forms of IM are more favorable in the context of health care and crime prevention.

11. We found a similar reticence towards future functions of IM that are currently designed and developed:
    a. There is only a widely shared desire for more convenience in various forms of IM. This did, however, not result in a support for possibilities of one tool that covers every possible IM function, again with the exception of health-care functionalities;
    b. Other desires for specific functions of IM were diverse and particular to smaller groups of our research respondents;
    c. While all research participants expressed desire to have more personal control over their forms of IM, in terms of, for instance, being better able to find them, or ‘reading’ their data themselves, this was stronger among vulnerable groups;
d. While all research participants expressed strong desires for more convenience and the possibility to personalise their IM means, this was stronger among elite groups; e. The high diversity among our research participants suggests there will be no single solution that satisfies everyone. Instead, future functions and forms of IM should be designed in an inclusive, value-sensitive way that accommodates individual and cultural differences, and that puts user needs first.

12. As far as future governance of IM is concerned:
   a. we found desires for transparency and legitimacy of procedures and practices, and for individual control over and choice of IM;
   b. we found taboos regarding monetization and a concern that in the future privacy and data management may become dependent on one’s financial resources;
   c. many of our research participants stressed people’s individual responsibility for the security of their personal data and their privacy;
   d. we found that taboos and desires for the governance of IM is partly contingent on cultural values and ideological beliefs, but also that these desires and taboos produce independent divisions between people.

13. Our data about future forms, functions and governance of IM, and especially the recurring desires for control over and choice of one’s IM suggest strongly that individual agency should be a part of our thinking about people’s engagement with future forms, functions and governance of IM. In particular, we propose that it is important to consider what people are invited or expected to do when they identify or authenticate themselves, and how much choice and control they have in such acts of IM;
   a. People find situations in which they have no choice or control over what they are asked to do often unpleasant and experience them as acts of submission;
   b. When people willingly hand over some control over their identity and personal data in order get something back, they are involved in (acts of) transaction, and the appreciation of transactions in IM tends to depend on how the tradeoff between take-and-give is assessed;
   c. Some acts of IM enable personalised expressions of identity, most notably in social media applications, but also in seemingly marginal options to choose one’s own bank card cover. Our outcomes regarding personalisation and choice, however, suggest that such acts of
expression are highly desired in IM.

14. Our outcomes give clear directions for research, design and policy:
   a. For new IM design, our data turns us into the direction of inclusive, user centric design;
   b. For regulation and governance of IM, our research indicates a clear role for national and international governments to provide and protect citizens’ control over their own data, and for providers of IM to be transparent and offer control to their users;
   c. For academic research we suggest that the importance of different kinds of agency made possible or prevented by specific practices of IM should be further investigated.
On an average day, we may draw cash from an ATM machine, we could run errands and use a Tesco card, or we might want to go to the cinema and pre-book our tickets online. On a less common day we could go on holiday and cross the border, get a check-up at the hospital or apply for a license to start a business. In all these cases we have to tell the particular organisation we deal with who we are. Pincodes, loyalty cards, passwords, a passport, patient cards and a national insurance number are only some of the means we have at our disposal to do so.

Ever more often our ‘things’ also want to know who we are: our mobile phones may be pincode protected, our laptops won’t start unless we scan our fingerprint and new cars can be biometrically secured. In the not so far future, our smart homes will recognise our faces and give us personalised access to, for instance, the kitchen, fridge and bathroom. The emerging internet of ‘things’ connects us to all these devices and to the outside world, providing us with a network of endless possibilities, yet only if we are able to consistently identify ourselves at its different entry points.

Consider, in addition, that the internet and social media in particular, have enabled us to reach out to many more people than before; family, friends and colleagues but also to people we have never met. We seek them to make new friends, play a game or share a hobby. Smart phones and the rapidly growing offer of apps make it possible to extend such contacts offline. Skout, Grindr and DateMe, for instance, all offer a location based possibility to meet new people. While anonymity and identity play can be part of the fun, most people appreciate authenticity and sincerity in such situations; hence, we and our new friends again need to identify ourselves in a trustworthy way.

While there are good reasons for such increased demand for identification and authentication (higher security, greater efficiency, better service, more fun and so on), these procedures are simultaneously sources of stress, ranging from concerns about privacy to irritation about long queues at the border or despair about lost passwords and pincodes. Nevertheless, in our current societies it has become near to impossible to be a citizen or a consumer without having a valid means to show and prove who you are.

Hence the reliable, trustworthy and efficient management of offline and online personal identities is rapidly becoming a key challenge for individuals, as well as a significant issue in social policy and economic development. In fact, different
national and international agencies have pointed to identity management - as the identification and authentication of identities towards institutions, things and other people, are usually called - as one of the main private and public challenges of the future (e.g. Camenisch et al., 2011; OECD, 2011; Gartner, 2012). It is also an issue that is subject to intense public controversy and contestation, especially with respect to access to, usage and ownership of the personal data required for identity management (cf. Bennett, 2010). In the UK in 2009, for instance, the government abandoned the national ID-card scheme as a result of unresolved concerns around privacy and data protection (Whitley and Hosein, 2009). Likewise, in the Netherlands, the national electronic patient file was cancelled after wide public protest (Boonstra et al., 2008), and several states in the US have developed legislation against the forced micro-chipping of persons (California bans, 2007).

IM is rapidly growing into a field consisting of a wide range of government and corporate actors, of privacy organisations and commercial consultants, of concerned journalists, systematic researchers and specialised lawyers. They develop, discuss and examine practical solutions for IM: across continental Europe governments are implementing E-identity cards; networks and associations of IM professionals, both national and pan-national are emerging rapidly; sectors like education and leisure are using new means of identification and authentication, like biometrics or smart wristbands, to facilitate their services. In this exploding field, it is relatively unclear how the main users of IM - ordinary people in different situations - engage with these innovations. On the surface, they manage their identities in very paradoxical ways: they are greatly concerned about identity theft and identity fraud, but they are sloppy when it comes to securing their pincodes and passwords; they don’t mind sharing much of their personal information through customer loyalty cards, but get upset when a government wants to introduce a compulsory national ID-card; they are eager adopters of LinkedIn but hesitate when it comes to an electronic patient file (see for instance Acquisti and Gross, 2006).

It is this key paradox, of sharing one’s identity in one situation while protecting it in another that we investigate through the IMPRINTS
research. We focus in particular on the taboos and desires that people have with regards to future means of IM such as biometrics, smart cards and wearables, alternatives to password authentication, or ID-implants. We have asked both the general UK public and specific elite and vulnerable groups what they know about future means and challenges of IM; how they perceive this; how it makes them feel; if, how and why they will adopt particular forms of IM; what their concerns and taboos are; and what their desires are. We have collected data through a variety of standard and experimental academic methods, ranging from focus groups, diary writing and interviews, to survey games, hackJams and performance art. In the following sections we first give a broad review of existing research into these issues. Then we explain our methods of data collection and analysis in more detail.

We subsequently present the responses of the public(s) under four headings: current everyday practices of IM; (dis)engagement with particular new forms of IM; desires and taboos with respect to new functions of IM; identification of new issues for governance of IM. We conclude with recommendations for design, governance and research.
‘Identity management’ is a term that is widely used in government and corporate circles, but it is not a term that occurs as standard concept in research and academic literature. Instead, the research that is relevant for our questions has occurred under the labels of ‘digital identity’, ‘electronic identity’, ‘authentication’, ‘identification’, ‘personal data’, ‘privacy’ or - sometimes - surveillance and sousveillance. Furthermore, while people’s views on specific means of new forms of identity management - e.g. biometrics, single-sign on authentication, smart wearables - have been analysed, the focus of this research has been somewhat unbalanced, and the approach limited, as we will explain later. Evidently, there are, in addition predictable differences between the theoretical approaches of specific disciplines, and the methods they use to explore user experiences and expectations. A complete overview and meta-analysis of the existing research is outside the scope of this report, in what follows we review the general trends on which the questions and approaches in our own research is built.

2.1 Concerns and attitudes towards (online) privacy

This line of research usually revolves around the following questions: which kind of data do people consider private; who is asking for this information and is this a trustworthy partner; in which context is this data asked for; is the information requested appropriate for the service or product provided? It has been carried out in a context of strategic questions for commercial and governmental registration and authentication. It is mostly aimed at understanding how and why people want or don’t want to share their data online so that impediments to the further development of e-commerce and e-government can be removed (e.g. Udo, 2001).

2.1.1 What do people consider ‘personal data’?

All research about this question points in the same direction: people consider financial, medical and civic (passport or national insurance number) data as their most personal and sensitive information, while hobbies, website visits, nationality, gender and age are considered less sensitive. There is a bit more variation with respect to one’s fingerprints and other biometric data, one’s pictures, name and address, purchase behaviour, media use and one’s social media posts: some people find these highly personal, others don’t (BGC, 2013; Cranor et al., 2000; Eurobarometer, 2011; InfoSys, 2013). There are also suggestions that socio-demographic features matter for one’s perception of personal data: high level of education, high use of the internet, high social status, and financial viability all
go together with considering your medical, financial and civic data personal.

2.1.2 Who can be trusted with your personal data?

Here too, existing research shows similar patterns: trust in organisations is a key factor for people’s willingness to share their personal data. Such trust depends on the organisation being known and trusted offline, on being a well-known, reputable organisation. Health organisations and banks come out as most trusted organisations, and internet and phone companies, as well as search engines and social network sites as least trusted and even as a threat to privacy (ACMA, 2013; BCG, 2013, Eurobarometer, 2011).

There is a less clear picture when it comes to trust in government; while the Eurobarometer (2011) finds in general that public authorities and institutions - including the European Commission and the European Parliament - are trusted more than commercial companies to handle personal data, their data for the UK shows considerably less trust in government and the EU institutions. Infosys (2013) suggests, in addition, a higher confidence of UK respondents to share their data for the purpose of online shopping than in online health.

2.1.3 What is the context of the personal data exchange?

This part of the research is less well developed and has produced different kinds of results:

PLACE: The Eurobarometer (2011) shows that UK citizens are much less concerned with the monitoring of personal data (surveillance) when it happens in public spaces than when it happens in private spaces (clubs, restaurants). Infosys (2013) also points at the importance of place, and demonstrates that people are willing to give up some privacy if they get bespoke commercial offers from their local retailers.

TIME: Smith and Lyon (2013) compared attitudes to surveillance across time, and found many changes in attitudes towards privacy and surveillance, although not all of them moving in the same direction: for instance while people in 2012 reported less knowledge about surveillance technologies and data laws than in 2006, they said to feel they were more in control over their data.

SECTOR: Research has also shown that privacy concerns differ across the particular field or sector in which personal data are exchanged: work place privacy, for instance, is perceived differently than travel privacy. In the latter context, privacy intrusions are thought to be more acceptable than in the work place (e.g. Nissenbaum, 2009).

2.1.4 How is personal data collected and is it appropriate to its purpose?

BCG (2013) distinguish between methods of data collection of which the user is aware (voluntary or compulsory disclosure), and of which the user is unaware (tracking and mining). Typically, users are less
comfortable with tracking and mining techniques that are not revealed to them: while people want to give active consent to websites using their data, they also feel they have only partial control over the information that, for instance, social networking sites and online shopping sites collect about them (Eurobarometer, 2011). Their concern about this increases with the sensitivity of the data involved: for health and financial data they would like an opt-in system where they have to give active consent (BCG, 2013). Phelps et al., 2000 similarly find that the kind of data that is shared, and the amount of control that users have are paramount in understanding their sharing behaviour and privacy concerns. Joinson et al.’s (2006) study, furthermore suggests that data storage is an additional factor for privacy concerns, with central storage raising more worries that personal or decentralised storage of data.

However, these considerations are modified by the purpose of data collection. If the purpose is the reduction of criminal or terrorist threat, people’s privacy concerns seem to wane. Infosys (2013) finds, as an example, that most customers (more than 82%) are comfortable with their banks mining their data in order to prevent identity fraud and theft, but less of them (about 51%) appreciate such mining if it is for the purpose of offering new services and products. Yet, within such a security context there is still a diverse appreciation of data collection methods (Sanquist et al., 2008).

### 2.1.5 Do different people have different privacy concerns?

Several socio demographic and personality features of individuals have been analysed to determine which of them influence attitudes towards privacy. The outcomes of these studies are contradictory.

**AGE** has been found to matter in different ways with both younger and older groups identified as not too concerned about privacy (e.g. Hoofnagle et al., 2010; Sheehan, 2002).

With respect to **GENDER**, Hoy and Milne (2010) find both more concern and more protective behavior among young girls using Facebook; in contrast Sheehan (1999) finds men to be more protective of their online privacy, while Kolsaker and Payne (2002) find hardly any difference between women and men.

**NATIONALITY** does make a difference for privacy concerns, due to different cultural values and internet experience (Bellman et al., 2004; Eurobarometer, 2011), but again not in a unidirectional and consistent manner.

Bansal et al., (2010) argue that personality traits, information sensitivity, health status, prior privacy invasions, risk beliefs, and experience all make a difference for the trust people express towards providing health information online. Junglas et al., (2008) zoom in on the big five of personality traits and find that agreeableness, conscientiousness, and
openness to experience each affect concerns for privacy.

2.1.6 Conclusion

The extensive research about concerns about privacy shows how different and interacting factors influence people’s concern for privacy and (hence) their willingness to share personal data. Apart from a range of as yet undetermined socio-demographic and personal features, a combination of situational variables also make a difference: the type of personal data involved; the trustworthiness of the organisation handling data; the methods and purpose of collecting personal data; and the context in which it takes place. While the combined results, thus, can only produce situational assessment of privacy concerns, there are a number of general tendencies that come out of most studies:

- that financial and health data are considered highly sensitive, but the organisations asking for them (banks and health care) are also among the most trusted ones;
- that some of the least trusted organisations (social media, online shopping) handle some people’s most sensitive data (status updates, financial information);
- that data collection for the purpose of fighting crime and terrorism is considered less problematic in terms of privacy concerns than data collection for other purposes;
- that people are willing to share their personal data, provided that they have control over how and with whom these are shared, and that there is a well-balanced trade off with the service rendered in return.

2.2 Accepting new technologies of IM

Current methods of identification and authentication come with a range of usability challenges: cards proliferate, passwords and pins are forgotten. In the past years a range of alternatives have been suggested: some of them are becoming common practice, such as biometrics, smart cards and single-sing-on services. Others are still in the research and design phase, such as graphic, visual, audio or colored passcodes; wearable technologies; or ID implants. There is an emerging body of research about the perceptions, attitudes and intention to use these new ID technologies.

2.2.1 Biometrics

In the past years, a number of studies have been published in which research is reported about people’s perceptions, acceptance and usability of biometrics. A dominant approach in these studies is the Technology Acceptance Model (TAM, e.g. Al-Harby, Qahwaji, Kamala, 2009; Chau, Stephens, and Jamieson, 2004; Giarimi and Magnusson, 2002; James, Pirim, Boswell, Reithel, and Barkhi, 2006; Krupp,
Rathgeb and Busch, 2013; Miltgen, Popovič and Oliveira, 2013; Morosan, 2011, 2012a, 2012b, 2012c; Rashed, Santos, Al-Eryani, Arwa, 2013; Rashed and Santos, 2010; Rodrigues and Santos, 2013). Some authors have used the notion of Biometric Acceptance Model (Ho et al., 2003; Chau et al., 2004) for studying the acceptance of biometrics but this concept has not been used widely. In the original TAM (Davis, 1989) the question is raised what will make users accept a new technology. Perceptions are key to understanding acceptance, especially perceived usefulness of the new technology and whether one thinks it is easy to use. Subsequent criticism and adaptations of the model have led to two additional factors being stipulated as relevant to acceptance, i.e. social influence and facilitating conditions. This extended model is known in the literature as the Unified Theory of Use and Acceptance of Technology (UTAUT, Venkatesh et al., 2003).

While most studies using this model find that the perceived ease and usefulness of biometrics (a range of biometrics have been studies) are indeed factors for people to consider further usage, a range of other factors have been identified as equally or even more important especially those concerning trust in the technology and the provider, and the risk for a user’s privacy (see, e.g. Miltgen, et al., 2013). Byun et al., (2013) analyse how people weigh perceived benefits against perceived risks of biometrics and conclude that the balance between the two will define the consumer value of biometrics. El-Abed et al., (2012) similarly observe that the perceived trust and robustness of biometrics against privacy attacks is an important factor for acceptance. James et al., (2006) have added that the physical nature of biometric also necessitates awareness of the corporeal invasiveness of the technology; they found in their user study that this is indeed an additional factor influencing acceptance. Morosan (2011, 2012a, 2012b, 2012c) adds that perceived innovativeness of biometrics also makes a difference for its acceptance, a claim based on her studies of users of biometrics in hospitality contexts. While these additions are beginning to add up to considering the a much wider set of perceived characteristics of biometrics as factors influencing its acceptance than in the TAM and UTAUT model, they also show the limits of this approach. Currently, these kind of studies have produced a range of differently defined concepts and instruments to measure perceived characteristics of (various) biometrics, but this has not added up to a systematic understanding. It is, in this respect telling that Alhussain and Drew (2012, p. 188) conclude after their readings:

“The review of the relevant literature on the technology adoption factors did not lead to any hypotheses, but rather helped to enhance awareness of the existing factors.”

The problems in the studies of user acceptance of biometrics have been identified in a more general sense for the
overall TAM approach which has been criticised for a lack of theoretical and methodological coherence (cf. Benbasat and Barki, 2007). Moreover, there has been little attention for the way the different acceptance factors play out against socio-demographic, psychological and cultural differences between users (but see Al-Harby et al., for a rare study of gender differences). In addition, the TAM approaches have been criticised for rationalist assumption that human behaviour is based on a systematic cognition and comparison of advantages and disadvantages. In that sense, TAM demonstrates many of the problems of other rational choice theories (e.g. Green and Shapiro, 1994), and seems less suited to capture everyday contexts and emotional, cultural or ideological factors affecting acceptance. The study of Byun et al., (2013) which identifies the perceived enjoyment of using biometrics as a key factor for potential and current users is a notable exception in this respect.

2.2.2 Smart cards

With the introduction of smart ID-cards in various countries and various context, some research has come up examining acceptance patterns. These studies are much less numerous than the biometrics acceptance studies but here too TAM based approaches are prominent (Chan et al., 2010; Loo et al., 2009; Plouffe, Hulland & Vandenbosch, 2001; Yeow and Loo, 2009); more qualitative approaches use field observations (Paul et al., 2011) and focus groups (Harbach et al., 2013).

Many studies show that potential or new users of smart cards tend to have little knowledge about the card and its particular functionalities: Al-Awali and Al-Amer (2006), for instance, find that young people in Bahrain were not aware of the impending roll-out of a National Smart Card; Loo et al., and Yeow et al, observe in their studies about the MyKad, the multipurpose smart card for Malaysia, that few people understood its use possibilities. Such users would appreciate a trusted third person to explain the usage and benefits of the card more clearly to them (e.g. Harbach et al., 2013; Paul et al., 2011). Some studies suggest in this respect that suppliers of smart cards do not pay enough attention to service, marketing and guidance when introducing the card to the market:

Surprisingly, after spending a very large amount of money on deploying an eID scheme, these factors were neglected by the German government and consequently the beneficial technical properties, such as the privacy-preserving nature of the card’s authentication facilities, did not receive public attention (Harbach et al., 2013, p.17).

Most of the studies are not of sufficient breadth or quality to be able to assess what the appeal of a smart ID-card is for future users. Al-Awali and Al-Amer (2006) present descriptive survey data only to suggest that 88% of Bahrain students are willing to replace their different bank and civic cards with one overall smart card; similarly, Arami, Koller and Krimmer (2004) report student survey data suggesting an overall positive attitude towards one
multipurpose student smart card for the University of Vienna, and that a smaller percentage would also appreciate the integration of such a card with off-campus bank and citizen applications.

In the most elaborate and sophisticated study of this body of research, Chan et al., (2010) apply a UTAUT model to the replacement of the old Hong Kong ID card with a compulsory new smart card. They surveyed 1179 people before and after their adoption of the new smart card, and found that their satisfaction with the card develops following one of two paths: a high trust in government coincides with great expectations and a higher satisfaction in using the smart card; people who expect to have little problems in using the card and are convinced of its convenience also report higher levels of satisfaction.

2.2.3 Alternatives to passwords

Passwords and pin codes are notorious for their problems of security, memorability and abundance: passwords can be hacked, they can be forgotten or one can have too many of them. In the past years, various alternatives have been suggested and explored; from single-sign-on services, to using Facebook and Google passwords for third-party services, to ‘pass-pictures’, ‘pass-colours’, ‘pass-sounds’ or ‘pass-songs’, to secure questions. The research about acceptance and desirability of these alternatives is relatively scarce and diverse.

With regard to single-sign-on Sun et al., (2011; 2013) find that SSO often fails to provide an improvement to people’s password management strategies; in addition they tend to misunderstand how single-sign-on works and have concerns about privacy and data security impede on user acceptance and satisfaction. Herath et al., (2012) similarly identify the possible risks of email authentication services as an impeding factor for wide acceptance. A particular form of single-sign-on comes from services that allow users to login with their Facebook or Google account details. This provides enhanced ease of access, but also involves linking websites through one account, which facilitates online monitoring and tracking. Both Bauer et al., (2013) and Egelman (2013) find that users are concerned about the latter but nevertheless do not pay much attention to privacy statements and the personal auditing tools that Facebook and Google offer.

Moving away from letters and numbers, there has been some research about the usability and acceptance of other types of codes, specifically graphical ones. De Angeli et al., (2005), conclude on the basis of two user studies that graphic pass codes
only lead to memory improvement if they are well designed. Moncur and LePlatre (2007) compare the recall of multiple pass words and multiple graphic authenticators and find that the latter are better remembered. Nicholson et al., (2013) compare the recall of face based and picture based pass codes by younger and older people, and found a general better performance by younger people. Faces seem to be better remembered by older people, as opposed to pictures by younger people.

Finally, there have been a couple of preliminary experiments with pass songs (Gibson et al., 2009) and pass colours (Isla et al., 2008). The methodology and outcomes, however, are inconclusive.

2.2.4 Smart wearables

There is a significant movement towards smart wearables, i.e. clothes, jewellery, watches or shoes equipped with sensors and/or rf id chips, and there is some research about people's expectations and acceptance of these. Anderson and Lee (2008), for instance, find that users judge an iPod jacket on the basis of its convenience and compatibility, while observability and social prestige (the ‘cool’ factor) are less important. Turhan (2013) finds, somewhat in contrast, that perceived usefulness of smart textiles is not an independent factor for their acceptance; rather a structural set of beliefs underlies the appeal of smart wearables. Duval and Hashizume (2005) examine the perception of prototyped cyberclothes, and find general interest in the comfort, safety and communication possibilities of such garment among members of the French public, especially among men.

While designers have experimented with making wearable forms of authentication (see Wilson and Flores, 2013), there is no research that focuses on the public’s engagement with such particular forms of authenticating or identifying jewellery, watches, and clothes.

2.2.5 Conclusion

There are a number of studies that have looked into the perception and acceptance of future means of personal identity management, whether identification or authentication. They have focused on distinct technologies, in particular biometrics, smart cards, alternatives to passwords, and wearable authenticators. There are no studies that compare the desirability of the different technologies to each other. The reviewed studies, especially those about biometrics and smart cards are dominated by varieties of the Technology Acceptance Model, which foregrounds the cognitive appreciation of advantages and disadvantages of a new technology, especially perceived usefulness of the new technology and whether one thinks it is easy to use. TAM has little attention for cultural and emotional factors affecting technology acceptance. In addition, there has been little systematic attention for the context in which the technology is used, and for the socio-demographic features and the lifestyles of its users. Sometimes gender and age have been incorporated into the
design, and there have been one or two studies that have incorporated questions of lifestyle and ideology into their background variables. In terms of methodological rigor and sophistication, the field is rather weak, with many small (student) samples, simple descriptive statistics and often limited prototype testing. Within the TAM paradigm, the field would benefit from a meta-analysis of the studies about biometrics (the only topic that has produced enough studies to do so), and from more sophisticated and theoretically informed hypotheses. More generally, the field would benefit from a wider and more open understanding of everyday IM practices, of the cultural and emotional factors that affect the desire for and resistance against of new IM technologies and of way use context and user characteristics make a difference. This is what our research among members of the public tries to achieve.
In order to solve the key paradox of IM, that people eagerly share their data in one context and anxiously protect them in another, and acknowledging that this is partly affected by:

- the type of personal data involved;
- the trustworthiness of the organisation handling data;
- the methods, purpose and context of collecting personal data;
- the perceived efficiency, ease and reward of sharing one’s personal data;
- a number of personal characteristics.

We ask the following questions:

1. Which means of IM do members of the UK public currently use to identify and authenticate themselves?
   a. which pleasures and problems do they experience with these means?
   b. how do these differ for use context and user characteristics?

2. Which desires for and taboos against future forms of IM do members of the UK public express?
   a. How do these differ for use context and user characteristics?

3. Which desires for and taboos against future functions of IM do members of the UK public express?
   a. How do these differ for use context and user characteristics?

4. Which desires and taboos do members of the UK public have for the governance of future forms and functions of IM?
   a. how do these differ for use context and user characteristics?

Given the wide and open reach of these questions, we conducted eight research projects differing in terms of design (standard academic versus creative exploratory designs) and means of data collection (quantitative and qualitative). These are summarised in Table 1.
Table 1  Sub-studies in the research

<table>
<thead>
<tr>
<th></th>
<th>General public</th>
<th>Subgroups</th>
<th>Which question?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Survey games</td>
<td>N=1000</td>
<td>1,2,3,4</td>
</tr>
<tr>
<td>2</td>
<td>Focus groups</td>
<td>12 focus groups</td>
<td>2,3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 intergenerational</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>workshop</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Q-sort</td>
<td>Experts, Students</td>
<td>2,4</td>
</tr>
<tr>
<td>4</td>
<td>Interviews</td>
<td>RFID Implantees</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Delphi</td>
<td>Experts</td>
<td>2,3</td>
</tr>
<tr>
<td>6</td>
<td>Cultural probes</td>
<td>Professional women</td>
<td>1,2,3</td>
</tr>
<tr>
<td>7</td>
<td>HackJams</td>
<td>Design students</td>
<td>2,3</td>
</tr>
<tr>
<td>8</td>
<td>Art performance</td>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>

Full detail of each study is in the respective publications (see Appendix 3).

We chose for a combination of designs and methods because of the challenges produced by researching future IM technologies. As Mancini et al., (2010) have noted, different representations of future technologies will elicit different responses, and research needs to cast a wide net in order to get the whole spectrum of expectations, especially when dealing with controversial technologies. We decided therefore on a triangulated approach, in which different means of exploration are brought together to get the best and most detailed idea of the concepts under study. The additional benefit is that the quality of one’s conclusions is enhanced by triangulation. To be more precise, our design involves the four basic forms of triangulation (cf. Denzin, 1970).
Table 2  Forms of triangulation

<table>
<thead>
<tr>
<th>Theory-triangulation</th>
<th>We used psychological, cultural, sociological and governance theories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method-triangulation</td>
<td>We gathered quantitative data (survey); textual data (focus groups, q-sort); visual data (hackJams, cultural probes)</td>
</tr>
<tr>
<td>Data triangulation</td>
<td>These data were gathered from the general public, and from specific elite and vulnerable groups</td>
</tr>
<tr>
<td>Investigator triangulation</td>
<td>More than one researcher was involved in analyzing and interpreting the data</td>
</tr>
</tbody>
</table>

In all studies (except for the art performances) participants were either confronted with visual stimuli representing future IM scenarios (as pulled from our earlier scenario sourcing, see Van Zoonen et al., 2012), or asked to create such future scenarios themselves. Moreover, the studies were designed to enable comparisons between contexts and users, and to tap into different kinds of arguments and feelings. Each sub-study was subject to its own appropriate methods of analysis and reporting, and published in different academic outlets (see Appendix 3). Here we present the general tendencies in our data under four headings:

- Current practices of IM
- Future forms of IM
- Future functions of IM
- Future governance of IM
The question that we will answer in this section concerns the means of IM that members of the UK public currently use to identify and authenticate themselves, paying attention to the pleasures and problems they experience with these means, and the differences between context and user characteristics.

### 4.1 Usage

For the general public in the UK, passport, driving license and bank cards for offline identification and authentication, and pincodes and passwords for online transactions are standard means of IM. Secondary means of IM concern loyalty cards, birth certificate and other civil register information, and tax or utility bills. On average, people have about 17 different means of IM at their disposal, mostly token or memory based. People don’t seem to have many problems handling these means; a considerable number of them report minor issues such as losing cards, misplacing them or getting them damaged. Only about five percent of the respondents in the survey said they had experienced serious card theft (of money or their identity). A similarly unproblematic picture emerges from people’s management of their passwords and pincodes; people claim to have no problems remembering them and only a few respondents indicate that they have to look them up again and again. Some keep them externally (written down offline or online). The usage of an online password management service is rare among the general public. As far as experiences with biometrics are concerned, these are by and large limited to airports, where people go through body scans or have their iris scanned. Travel to the US was mentioned specifically as a situation where one is subject to biometric authentication.

We found that identity management is strongly stratified, meaning that socio-economically vulnerable groups who spent relatively little time in education have fewer means of identification than strong socio-economic groups with a longer education history. Other standard demographic variables like age, gender, household size or ethnicity do not seem to make a difference for the number of IM means that people have.

### 4.2 Problems

In contrast to the general public, the elite groups in our research (professional women, experts) do report annoyance with passwords; they say they have too many, have trouble managing and remembering them and find the recurring online requests for identification and authentication irritating, frustrating, and not always necessary. A similar picture
of annoyance occurs among these groups when it comes to travel security, which is considered repetitive and time consuming. However, these groups also feel they have little other choice than to submit to the password and travel security regimes, since there are no alternatives to acquire the services, products, access or border crossing involved. These issues have little to do with actual difficulties in using IM technologies, but rather the feelings evoked by these unavoidable acts of identification and authentication are the problem. In terms of agency, these experiences suggest a feeling of submission to the respective systems, rather than a perception that one gets something valuable back which would be perceived as transaction.

Our vulnerable groups report somewhat more tangible problems with their means of identity management: for the elderly the recollection of passwords and pin codes is an issue that is increasingly insoluble. Hence, they often share these with family members or caregivers in order to maintain access to their accounts and services. Refugees sometimes talked about their authentication documents not being trusted by the authorities, or about their ID tokens getting lost. They therefore tended - uniquely among all people in our research - to prefer memory based systems of authentication.

Of all means of identification and authentication people use at present, only biometrics produce a set of concerns among some people that seem particular to the technology. Some people strongly associate fingerprint technology and face recognition with crime contexts and therefore don’t like the usage of these forms of biometrics in their own situations. Other people strongly feel that remote biometrics in particular are used without knowledge and consent of the people subjected to associate biometrics with state control and surveillance (face and gait recognition through CCTV for instance).

4.3 Pleasures

Few people explicitly reported pleasures of identity management; it seems in general our research participants take IM as an inevitable requirement of our everyday lives that may produce problems but does not belong in the realm of pleasures. However, a few means of IM are exceptional in this respect and stand out for how users appreciate them. Loyalty cards have the capacity to evoke pleasure among their users; women in our study reported that they like the immediate benefits, and that some of them make them feel as special customers.

A similar feeling of being special is reported by the early adopters of RFID implants that we talked to. Their implants enable them easy access to their digital devices, their home, car and a range of other possession. For some of these Do-It-Yourself Chippers the implant is not too different from an access card or a set of keys. They feel the implant is easy and efficient and considered the chip a tool to solve a range of everyday access and authentication problems they experienced in their everyday lives. However, for a
select number of them the chip is also an expression of them being technological forerunners and special, like the humanoids of the future (see Wagemakers, Van Zoonen and Turner, 2014 for more detail).

4.4 Discussion

Our inventory of the different means of identification and authentication that people currently have at their disposal, and the problems and pleasures they experience with them, suggest strongly that IM for the ordinary citizen or consumer is not much of an issue yet, neither in positive nor in negative terms. Our encounters with different groups and individuals did not indicate a sense of urgency around practices or problems of IM. While people regularly expressed a concern about cybercrime and a desire for the government and the police to do more against it, this did not result in highly reflective and secure procedures for themselves (see Van Zoonen and Turner, 2013). Evidently, some specific groups of people do experience problems with current means of identification and authentication which emerge from the feeling or the reality of having no control over the various technologies, and being subjected to the demands of state security or commercial systems. These issues, however, can hardly be generalised to a wider public.

In contrast to a somewhat uninterested and unbothered public, government and corporate actors are intensely active in discussing, developing and implementing new national, local, organisational or commercial systems of IM. This contrast inevitably reflects a mismatch between push factors of these actors interested in further introducing and refining IM systems, and the lack of a pull factor among neither a general public nor a specific one; members of various publics hardly experience a direct individual need or desire for it. It is against this wider background that we need to understand our outcomes regarding taboos and desires for future forms and functions of IM, and views about future issues for governance.
The question answered in this section concerns the desires for and taboos against future forms of IM among members of the UK public, and how these differ between use context and user characteristics?

Through the scenario analysis we identified a wide range of future forms of identity management, ranging from RFID implants to exceptional biometrics to smart wearables, multipurpose cards and graphic alternatives to passwords (see Van Zoonen et al., 2012). We selected a number of those for further discussion with members of the public, in particular RFID implants, smart tattoo, smart jewellery and other wearables, an implanted phone, QR codes and multiple purpose ID cards. By and large, our research participants did not like these innovations very much and expressed reluctance to use them.

5.1 Desires and taboos

From the different responses in the various research projects, we could distill a number of dimensions that matter for the question whether people desire or detest the future forms of IM that we discussed with them.

Familiarity - It became clear that innovations that are on the market already (GPS footwear, smart watches, Google Glass) were liked better than the more futuristic ones. It seemed that people were already somewhat familiar with those and could better imagine how to use, and - especially - personalise them. Evidently, familiarity with new IM technologies will differ among specific groups. In that respect it is telling that our older participants often expressed frustration or apathy towards these innovations because they did not know or understand them.

Good/bad taste - Nevertheless, familiarity does not automatically result in desirability. When confronted with the possibility of putting a QR code with personal information on your gravestone, many of our participants thought this was creepy and in bad taste. The notion of bad taste also came up regularly in responses to smart tattoos which evoked strong associations with Nazi camps, cattle branding or with chavvy, tacky low culture.
**FUTURE FORMS OF IM**

Safety - Another set of arguments used against the new forms of IM that we showed our participants concerned their assumed safety: smart jewellery could be lost, smart tattoos would be too visible and - like RFID implants - could be chopped off, etcetera. Yet, biometrics and ID or customer loyalty cards that are in principle subject to the same risks, did not evoke these fears, suggesting that such anxieties are caused by the novelty or the associations of particular technologies just as much, and maybe even more, than by their ‘objective’ risks.

Security - most of the new IM that we confronted our participants with evoked strong concerns about data security and privacy. We discuss this in more detail in Section 7.

Personalisation - It was also clear that some new IM technologies were liked or disliked because of the way they could (not) be integrated with everyday needs and practices. Technologies that can be personalised to one’s lifestyle were seen in a more positive light than the ones that didn’t. This led, for instance, to some groups of women liking smart jewellery, but others finding it problematic: they like to change jewellery with outfits, or to swap jewellery with friends. Likewise, body based technologies like implants or biometrics were resisted by people depending on the care of others, because they could not be shared.

Cool - some future IM technologies evoke enthusiastic responses because of their ‘cool’ factor: having and using a Google Glass, smart watch, jewel or other wearable is considered by some people as a sign of being up-to-date with the newest techs, and having the money to acquire them. In addition, biometrics is cool for some people because of its association with a cosmopolitan lifestyle. This cool factor worked for small and different groups among our research participants, particularly younger men for the high tech applications and younger women for the smart jewellery.

5.2 Differences between users

While our different research data did suggest differences between users, these were differences of degree of disliking the new technologies, rather than differences of kind. In other words, there were no groups who expressed strong desires for innovations in IM, there were only groups that were less reluctant than others. There was a predictable age difference with younger groups less negative (but still negative) than older groups. Heavy usage of smart phones also meant a less negative perception, but other types of
media usage did not make a difference. In terms of life styles and cultural values, a high trust in government and politics also meant less hesitance towards innovations in forms of IM. Our data also showed that particular domestic situations are relevant for the reluctance towards new forms of IM. In extended or joint families, future IM technologies were assessed on the basis of their sharability. For the elderly in those and other care situation, it needs to be possible that their (new) forms of IM can be shared with others.

5.3 Differences between context of use

There appeared to be two contexts in which a number of IM innovations are more easily accepted and those are the medical/health one, and the crime prevention one. 70.3% of the survey respondents, for instance, expressed a desire to have all their medical information on one card. From the focus groups health came up similarly as a ‘privileged’ context for innovations in IM. People find RFID implants, for instance, acceptable for purposes of health monitoring and tracking. They similarly can imagine the usefulness of an RFID jewel (also because identification bracelets already exist) for people with special health care needs; in case of emergencies it is easier to access one’s medical details.

With regard to crime prevention, it is important to note that our research participants are concerned, in particular, about increasing issues of identity fraud and would not seem to mind additional IM measures to prevent it. Interestingly, as we observed a couple of times already, this does not lead to more secure individual behavior, but it does lead to a heightened call on governments and organisations to provide more security. The appreciation for more intense IM procedures in the context of terrorism prevention is especially high in the immediate aftermath of terrorist attacks, but wanes with time, as we saw in the literature review.

5.4 Discussion

Since most of our research participants do not experience many urgent problems with their forms of IM, it should not come as a surprise that the future forms we presented to them do not evoke much enthusiasm, on the contrary. There seems to be little added value of these novelties for them, and they consider many of them as unsafe and at odds with their everyday practices. There is, in addition, also a strong role for the expressive and narrative dimension of these new technologies. The fact that a small number of our participants are attracted by the ‘cool factor’ of some of the new IM tokens suggest strongly that for some groups, especially the younger ones, a particular form of IM can thus also function as a marker of a desirable lifestyle. Yet, the reverse is also and more strongly present in the wide rejection of body based innovations like smart tattoos and RFID implants; those technologies tend to be seen as expressions of an undesirable past (smart tattoos remind people of the Holocaust), of a questionable social position (smart tattoos as expression of lower class taste) or as objectionable
dehumanisation (people associate RFID implants with chipping pets).

The fact that that familiarity is also an important dimension in the reactions to the new IM technologies suggest that there is possible little cultural and psychological space to experiment with forms of identity management that do not build on people’s existing practices and expectations. For most people token based IM is what they grew up with, memory based IM is what they have become used to. People are somewhat familiar to biometrics in contexts of travel security, but would possibly be hard convinced that biometrics offer an alternative to the token and body based means of IM that dominate other contexts, especially because they are not unhappy with the latter. A possible recommendation following from these insights, is that successful innovation of IM builds on existing means and practices, rather than proposing completely different alternatives. Hence, enhancing rather than replacing may be the wisest advice.
While we thus did not find strong desires for new forms of IM, it could be that people would like their current means of IM to be better. We thus asked in various ways about desires for new functions of IM, such as having one card with which you can do everything, or having more simple ways of authenticating yourself online. Here too, a number of dimensions came out similarly from the different research projects.

### 6.1 Desires and taboos

**Convenience** - The main tendency among our participants was that they would like and expect IM to become easier and more efficient. This is consistent with the overall literature on technology acceptance that suggests ease of use is a crucial factor for the uptake of new technologies. While such desire for greater ease of use is general, it does not translate into a general desire for specific IM-technologies to create such ease, or for the replacement of all different forms of IM with one general one (but see Wagemakers et al., (2014) for an exception among small groups of Do-It-Yourself Chippers). While many participants in our research identified biometrics as providing easier, quicker and safer methods of IM, it was at the same time considered problematic by others (see Section 7 for more detail on different views on biometrics). Hence, a forced one-technology solution comes out as a taboo among our participants.

**Other desires and taboos** - Table 3 indicates a high diversity among our survey respondents with respect to other future functions of their identity technologies. The table shows that more than half of our respondents see clear possibilities for improvements of their current cards which would offer more ease and transparency of use (items 1,2,3); the two possible safety options on cards (to track one’s kids and warn against criminals) draw about a third of the respondents; the ‘social options’ for membership and customer cards are not very popular; neither are the suggestion to replace cards with one other IM instrument (a biometric, app, implant or jewel).
### Table 3  Future functions of IM

<table>
<thead>
<tr>
<th>I wish that in the future .....</th>
<th>% yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>I could have all my medical information on one card</td>
<td>70.3</td>
</tr>
<tr>
<td>I could read my own cards so that I knew where and when I used them</td>
<td>61.8</td>
</tr>
<tr>
<td>I could have a tracker on each of my cards so that I could never lose them</td>
<td>59.0</td>
</tr>
<tr>
<td>I could have one card with which I could do everything</td>
<td>42.5</td>
</tr>
<tr>
<td>My kids would have a card with a tracker on it so that I could monitor where they are</td>
<td>37.9</td>
</tr>
<tr>
<td>I like to have many different cards for different purposes</td>
<td>37.2</td>
</tr>
<tr>
<td>Credits on one customer card would add to those on the others</td>
<td>36.2</td>
</tr>
<tr>
<td>My cards would start beeping if there was a criminal nearby</td>
<td>34.0</td>
</tr>
<tr>
<td>We could get rid of cards altogether and replace them with a fingerprint or other biometric</td>
<td>31.8</td>
</tr>
<tr>
<td>I could 'pimp' my credit and customer cards so that they look more personal</td>
<td>28.8</td>
</tr>
<tr>
<td>My membership card would tell me that there are other members nearby</td>
<td>16.1</td>
</tr>
<tr>
<td>We could get rid of cards altogether and replace them with a body implant that contains the same information</td>
<td>12.4</td>
</tr>
<tr>
<td>We could get rid of cards altogether and replace them with apps on our smartphones</td>
<td>12.0</td>
</tr>
<tr>
<td>We could get rid of cards altogether and use smart jewellery or textiles instead</td>
<td>10.8</td>
</tr>
<tr>
<td>My customer card would tell me if there are other people in the store who have the same taste and preference as I have</td>
<td>8.6</td>
</tr>
</tbody>
</table>
6.2 Differences between users

Vulnerable groups

We found strong suggestions in our different research projects that social vulnerability is an important factor for desires for new functionalities of identity management. The lower income and lower educated groups expressed stronger desires for control over their means of IM; older people especially appreciated the idea of having all their medical information on one card.

Elite groups

People who need to identify or authenticate themselves regularly as part of their jobs, or of their travel patterns express stronger needs for easier ways and for one-tool solutions, than other groups. The Scottish professional women in our research, for instance, were interested in a smart jewel that would contain all their personal data and that would help them accessing online services and getting through the airport as well.

Attitudes and lifestyles

Biometrics and its functionalities clearly divide people along the lines of political attitudes and cultural lifestyles. The desire for easier means of IM plays out in a desire for biometrics among people with a high trust in state agencies like the law, police and secret service, with a conservative attitude, and/or a cosmopolitan lifestyle. The desire for more control is not limited to vulnerable groups, but is also found among privacy advocates.

6.3 Differences between context of use

In addition to a desire for greater ease of use, Table 3 suggests that there is also a general desire for IM technologies to contribute to better health. 70.3% of the survey respondents expressed a desire to have all their medical information on one card, and this desire was even bigger among older respondents. Our other data also suggest that health is a “privileged” context for innovations in IM: when given the example of being rushed to hospital people tend to find otherwise intrusive technologies like RFID implants helpful. From our in-depth conversations with older adults, it appeared that they framed new IM technologies as potentially useful for improved health care, and for their general well-being, remembering, and self-reflection. Yet, at the same time they were also worried about the possible privacy intrusions of, for instance, location-based-tracking devices (Thomas et al., 2013).

6.4 Discussion

There is general desire for more simple and efficient ways to identify and authenticate oneself, and this desire is even stronger among elite groups. Nevertheless IM solutions that are based on one technology (biometric, smart app or all-purpose card) are not very popular, partly out of fear of dependence, or security breaches, but also because such a
choice for one technology is at odds with current desires for choice and personalisation, and the importance of context for the desirability of particular IM solutions. Health appears to be a privileged context for the introduction of new and improved functionalities of IM: in matters of medical urgency, one-tool-solutions are seen as more desirable than in other contexts, especially among older people.

The high diversity among our research participants regarding their desires for future functions of their IM technologies suggests there will be no single solution that satisfies everyone. Instead, new functions (and forms for that matter) of IM should be designed in an inclusive, value-sensitive way that accommodates individual and cultural differences (see for more detail Briggs and Thomas, forthcoming).
Governance issues concern needs for future legislation, regulation and policies of governments, matters around corporate usage of personal data, and individual control of personal data. The personal, corporate and state governance of the personal data involved in different means and systems of IM is a matter of significant concern among all our users. The question is who gets to see your data, and what happens with them?

7.1 Desires and taboos

**Legitimacy** - privacy and data security concerns extend beyond particular forms of IM, and relate to various dimensions of the management of personal data. Our participants were concerned whether the levels of surveillance or intrusion in some systems was appropriate, whether data was acquired and stored at the right level and whether appropriate data segregation and ‘contextual integrity’ was maintained (Briggs and Thomas, forthcoming). Such concerns speak most strongly in association with biometrics, which for some is particularly associated with state power and control, crime and terrorism prevention and civil liberties infringements. Many of our respondents wanted separate data systems for separate purposes, with access limited according to purpose and consent. Nevertheless there was also a considerable group who thought that people who had nothing to hide had nothing to fear either.

**Choice** - In our different conversations with our research participants, it became clear that choice of identity technologies was an important dimension in their taboos and desires for the future. Many new functions were considered acceptable or desirable, provided people would be given a choice to adopt them. Compulsory functions were met with resistance. Informed consent and opt-out strategies were considered crucial for the future. In addition, choice should not be contingent on physical resources; people would argue against compulsory fingerprinting, for instance, that not everybody has fingers, or even hands.

Information about them is available online, and they would want to give active consent to the usage of their data. Some people feel that this is particularly relevant for biometrics, where it seems that each new development in remote biometric technologies takes away control from people, in terms of knowing when, where and why data are taken from them and used. A specific concern here is the control over one’s digital legacy, in other words, what happens to ones online profiles and data after death. Many of our participants were not familiar with digital legacy systems yet, and if they were they considered them as unusable, because of issues of control, information leakage, privacy breaches and the new threat of digital vandalism. That our digital afterlives are an as yet unresolved concern for many people, also came out of the fact that the majority of the creative exercises we invited our research participant to join in, focused on this challenge, either in the variety of living on or in the form of being forgotten (Gomez Flores, 2013).
Likewise, IM functions that requires a considerable financial investment of their users were met with reluctance; in fact, one of the main fears about future developments of IM was that they would come with considerable costs.

**Trust** - our research participants regularly recounted incidents in which data were lost or abused; such stories referred to both government and large corporations. The fear of identity fraud was strong, and it was considered one of the main crimes of the future that need stronger policing. People could clearly identify the groups of people that would have access to their identity information (family, close friends), and felt it should be only revealed to ‘appropriate’ people. A number of organisations and types of people were discussed as being untrusted, including the UK government and social network sites such as Facebook. Sometimes an organisation was trusted, but participants still believe disclosing information to them was risky, or perhaps their employees might not be trusted. Rather than citing specific groups who they would be comfortable sharing information with, people talked about the general importance of who would get to see their identity data. In addition, it was clear that ‘trust’ is also a personal feature, with people who have a high trust in state institutions (police, law) being less concerned about future developments than people with less trust. Here too, it became clear that people who tend to have a problematic relation with the state (e.g. refugees, ethnic groups) are also more suspicious of the legitimacy of new developments.

**Monetization** - There was general concern that the secure and safe management of personal data would become dependent on one’s financial resources; people expected that internet services, for instance, would become even more subject to advertising and that their control over their personal data would only be possible if they would pay for it. More than two-third of the survey respondents, for instance, agreed with the statement:

“The way things are going, we’re going to have to pay to retain any privacy on the internet in the future.”

*(Van Zoonen and Turner, 2013)*

**Personal responsibility** - People also felt they had a level of personal responsibility to be more careful with their own data, perhaps to counteract the lack of control they sometimes experience with new forms and functions of IM. Such sensible management made people feel more secure; some of our participants thought people who did not act cautiously invited their own data abuse.

### 7.2 Differences between groups

Our data suggest that cultural values and ideological beliefs are the main factors dividing our research participants with respect to their desires and taboos for the future governance of IM. A general trust in the state, for instance, carries into a more trusting perspective on future developments.
around IM governance. Socio-demographic factors and media-use patterns seem less important, with the exception of age; older people tend to want more governance reassurance than younger ones. In addition, governance beliefs about future IM themselves divide our respondents, as can be clearly seen in the way people respond to future developments in biometrics. We found four types of response to biometrics (Norval and Prasopoulou, forthcoming): privacy advocates, conservative techies, safety champions and casual adopters. Each one reveals a distinct understanding of biometrics and subsequently different ways through which people envisage incorporating biometric technologies into their everyday practices. Yet, it is unclear if and how these beliefs coincide with socio-demographic, media use and other social-cultural patterns.

7.3 Differences between context of use

While we did not ask specifically about governance issues in particular context, our overall data suggest that the contexts of health care and crime/terrorism prevention are areas where people are possibly willing to relax some of their concerns about legitimacy, control and choice. In the health context the general anxiety about connecting different databases is may wane under the pressure of life saving first aid; in the context of crime prevention, privacy policies may be considered less important, although - as discussed in the literature review - such tolerance tends to disappear with time.
Our study produced a mix of clear and tentative results.

To begin with, regardless of governmental, corporate and activist activity around IM, our data do not suggest that ordinary members of the public currently consider it a huge issue for their own everyday lives. When confronted with examples of the innovations produced by different stakeholders in this field, our research participants, generally expressed reluctance, sometimes in the form of wonder, other times in the form of clear disgust. Aesthetic and cultural preferences were clearly important for these reactions, as were social and political concerns regarding privacy and surveillance. Yet, if ‘hygiene factors’ (regarding legitimate and competent procedures of data management, cf. Briggs and Thomas, forthcoming) were taken care of, people became more willing to consider these innovations.

Secondly, our data do not suggest that people feel an urgent need for new means of IM. In general, people hardly report problems around their current means of identifying and authenticating themselves and - probably as a result - they also express little desire for actual new ID technologies or functions, with the exception of IM for health purposes. When probed, however, it is clear that people are concerned about the way future developments will be governed, with particular desires for institutional legitimacy of data management (referring to the procedures for data collection, segregations and access), for personal control and for choice. In addition, there is concern that such legitimacy might come to depend on one’s financial resources.

Thirdly, our outcomes within and between studies show such a great diversity of desires and taboos that it is clear that there is not a single problem with IM, neither is there a one-size-fits-all solution. Differences between users and differences between contexts are considerable and they do not tend to point into one easily understandable pattern, with the exception of differences between elite professional groups and specific vulnerable groups, who both have their own particular reasons and needs for improvement of their IM means and functions. The general diversity of desires and taboos for innovations of IM require that they are developed by using an inclusive and value-sensitive design approach that accommodates differences between potential groups of users (Briggs and Thomas, forthcoming).

Fourthly, we have produced a multitude of outcomes that define the necessary bottom line for innovations in IM and indicate some of the desires specific groups in specific contexts may have. We have not been able to empirically assess the underlying logic of these situations. We have, however, developed a more hypothetical understanding of underlying patterns, based on the strong desire for personal control of their means of IM that our research participants expressed.

This desire for control invited us to further discuss the possibilities for agency that are
present in current and future practices of IM (see Van Zoonen and Turner, 2014). In such agency-perspective, the decisive factor for people accepting or rejecting, loving or hating, desiring or fearing new forms of IM, concerns the possibilities they have to keep control over their identity and their personal data. If we then look at typical situations of IM we can distinguish three types of act that involved varying degrees of agency and control:

- in security checks and surveillance operations by the state we hand over our data (driving license, ID-card) with little control over the situation (we have to comply), nor over what happens with our data. In some cases we don’t even know that our data are harvested. We can consider these situations as involving acts of submission: while some situations are objective acts of submission (you have to show your driving license when asked by the police), others are mainly experienced as acts of submission but do, in fact, offer the opportunity not to oblige. It seems clear that when an innovation of IM is perceived or felt as an act of submission over which one has no control, it stands little chance of being widely accepted unless enforced by legitimate means.

- In most situations of identification and authentication we hand over our data in order to get something back: our money, products, services or access. These acts can be labeled as transactions and in such acts we willingly hand over some control over our identity and our personal data, because we get something back in return. If and how much people will appreciate such transactions depends crucially on how they assess the quality of the tradeoff between give-and-take in the particular transaction. For transactions, how people perceive the trade-off between give-and-take is crucial, as is increasingly recognised by the corporate sector involved in innovating IM practices and systems (e.g. BCG, 2013).

- And then there are the situations in which people are able to express their identity or identities in ways that basically suit themselves: we can understand these as acts of expression that take place, among others, through social media, but also through the creation of personalised images on bank or transport cards. Such acts of expression are rare in current forms of IM that treat people as carriers of data units, but the desire for such more expressive means of IM which, in a way, tell the story of a person, is present in the discussion we had with our research participants about the possibilities for personalised and more aesthetically pleasing means of IM. While it is also obvious that some people have little desire for anything more than quick, easy and secure means of IM, for others expressiveness is possible an important factor.
While particular industries have developed recommendations for governance of identity management within organisations and work flows, identifying particular roles and responsibilities (see e.g. Etges and Ruysam, 2011), there are relatively few recommendations that cover the everyday usage outside of IM schemes outside of organisations. The Imprints research has focused particularly on such everyday usage and concerns of mundane, non-professional users. Our recommendations follow from a principled position to put their interests first. This is in contrast to more general reflections on ‘identity ecosystems’ as proposed, among others, by the US government in its National Strategy for Trusted Identities in Cyberspace (2011)\(^1\) that are first and foremost inspired by visions of economic renewal. While user interests are certainly present in such visions, they are managed within the overall framework of (personal) data as drivers of economic growth. Such economic framework, however, comes out as one of the main concerns of our research participants, who feel their interests are likely to be subjected to those of ‘big business’.

Our recommendations are not necessarily new or original and many of them have been identified already in reflections on inclusive and user-centric design. The recommendations we present here, however, can be directly linked to specific research outcomes and are thus both empirically and ethically grounded.

9.1 Recommendations for designing, developing and implementing new IM systems

Our research among users has identified a number of specific do’s and don’ts that can be summarised in one sentence: put the interests of users first.

\(^1\) http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
## RECOMMENDATIONS

<table>
<thead>
<tr>
<th></th>
<th><strong>DO</strong></th>
<th><strong>DO NOT</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User centric</strong></td>
<td><strong>Identify the particular needs, taboos and desires of the target user group</strong></td>
<td>Assume easy stereotypes about users, for instance, that youth will easily accept IM innovations</td>
</tr>
<tr>
<td></td>
<td><strong>Build on existing practices and experiences in the target user group</strong></td>
<td>Expect that your users will be innovation or gadget prone</td>
</tr>
<tr>
<td></td>
<td><strong>Realise which kind of personal data you are asking from your user group and assess whether these are part of sensitive data</strong></td>
<td>Expect that users will share their sensitive personal data for the benefit of an abstract social or organisational goal</td>
</tr>
<tr>
<td></td>
<td><strong>Consider if your user groups perceives your organisation as trustworthy</strong></td>
<td>Deny that your organisation might have a trust issue and thus needs to develop better practices</td>
</tr>
<tr>
<td></td>
<td><strong>Plan when and how to communicate with your target group of users</strong></td>
<td>Wait until the end of the process and then plan communication</td>
</tr>
<tr>
<td></td>
<td><strong>Include both rational, emotional and cultural messages in communication</strong></td>
<td>Limit communication to arguments about efficiency, ease or benefit for the organisation.</td>
</tr>
<tr>
<td></td>
<td><strong>Make personalised means of identification and/or authentication possible</strong></td>
<td>Force people to personalise their means of identification and/or authentication</td>
</tr>
</tbody>
</table>
9.2 Recommendations for regulation and governance of IM schemes

For governance and regulation of identity management, our research indicates a clear role for national and international governments to protect and promote the interests of citizens, consumers and other users of identity management schemes, leading to measures to:

- Inform and educate the public about general and specific issues around identity management, leading to more data literacy and secure practices among the public;
- Encourage providers of IM schemes to adopt transparent procedures and give users access to and control over their own data;
- Develop an identity management quality label that shows that the IM providers follow secure, user-centric and transparent procedures;
- Identify and provide additional services for groups that are vulnerable in terms of identity management (e.g. elderly, refugees, homeless);
- Develop regulation to resolve the issues emerging from having ‘digital afterlives’.

Providers of identity management schemes should:

- Always follow an opt-in strategy when sensitive personal data are concerned (e.g. health and finances); always provide an opt-out strategy for all personal data.
- Make sure that procedures of data collection and usage are completely transparent to users while avoiding lengthy and inaccessible privacy statements
- Enable users to control and correct their own data in an easy and accessible way.

9.3 Recommendations for further research

There are two types of recommendations for further research: one set concerns new directions with existing approaches regarding technology acceptance and privacy concerns; the other builds on our identification of IM as a particular type of act that involves varying degrees of agency, from submission to transaction to expression.

Within existing approaches to technology acceptance and privacy concerns:

- Conduct meta-analyses aimed at establishing which socio-economic, attitudinal or cultural factors are most important in producing different patterns of acceptance and rejection of IM;
- Explore situational and contextual factors as relevant predictors of different patterns of acceptance and rejection of IM;
RECOMMENDATIONS

- Examine a wider variety of IM technologies;

- Use more complex modelling techniques to measure the direct and interaction effects of socio-demographic, attitudinal, cultural, situational and contextual variables on acceptance or rejection of IM.

With respect to agency in IM:

- Examine in more detail how specific forms of IM are framed in different kinds of media by different actors (journalism, popular culture, blogosphere), include comparisons across time and place;

- Explore more systematically how particular IM technologies evoke feelings of submission, transaction or expression among members of the public;

- Use experimental designs to compare whether and how different levels of agency evoke different responses from members of the public towards particular forms of IM;

- Explore and test how expressive dimensions can be incorporated in the design of new forms of IM.


Hoofnagle, C. J., King, J., Li, S. and Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? Mimeo, Berkeley.


### A.1 Sources for more methodological detail

Basic information about the research methods is on the IMPRINTS website:  
[www.imprintsfutures.org/research-strands](http://www.imprintsfutures.org/research-strands)

More detail can be found here:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
## APPENDIX 2

### Research design

|---|---|---|
### Results

#### Scenarios


#### Published

#### Presented

#### Usage and users


<table>
<thead>
<tr>
<th>Table Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Published</td>
</tr>
<tr>
<td>Published</td>
</tr>
</tbody>
</table>
## APPENDIX 3

### Impact on government and parliament

<table>
<thead>
<tr>
<th>YEAR</th>
<th>DATE</th>
<th>WHO</th>
<th>CONTENT</th>
<th>ACTIVITY</th>
<th>TARGET</th>
<th>EFFECT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>November 18</td>
<td>AN-EX</td>
<td>Contribution about biometrics to public consultation by the Department of Education on Individual pupil information prescribed persons regulations.</td>
<td>Written evidence</td>
<td>Government UK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>December 5</td>
<td>LvZ-LU</td>
<td>Representing the Global Uncertainties Programme in the Research Councils’ Parliamentary Showcase for the House of Commons. Project announcement.</td>
<td>Exhibition</td>
<td>Parliament UK</td>
<td>Visibility to MPs and Minister of Universities and Higher Education</td>
</tr>
<tr>
<td>2013</td>
<td>January</td>
<td>PB-NU</td>
<td>Review for the UK Government’s Foresight Project <em>Future Identities</em>.</td>
<td>Written evidence</td>
<td>Government UK</td>
<td>Taken up in Foresight document</td>
</tr>
<tr>
<td></td>
<td>January 10</td>
<td>PB-NU</td>
<td>Presentation to Home Office Centre for Applied Science and Technology (CAST), London.</td>
<td>Oral presentation</td>
<td>Government UK</td>
<td>Visibility to civil servants</td>
</tr>
<tr>
<td></td>
<td>March 12</td>
<td>ALL</td>
<td>Presentation to Sandpit Stakeholders, Birmingham.</td>
<td>Oral presentation</td>
<td>Government UK</td>
<td>Reporting back</td>
</tr>
<tr>
<td></td>
<td>October/November</td>
<td>LvZ-LU</td>
<td>Supervisory Board Data Dialogues of Office for National Statistics and ESRC to examine public attitudes towards administrative data sharing.</td>
<td>Meetings</td>
<td>Government UK</td>
<td>Visibility, service</td>
</tr>
<tr>
<td></td>
<td>December 12</td>
<td>LvZ-LU</td>
<td>Presentation to the Knowledge Platform Identity of the Dutch government about the IMPRINTS research.</td>
<td>Oral presentation</td>
<td>Government NL</td>
<td>Taken up in further development and communication strategies</td>
</tr>
<tr>
<td>2014</td>
<td>January 23</td>
<td>PB –</td>
<td>Invitation to panel discussion on privacy and behaviour</td>
<td>Oral</td>
<td>European</td>
<td>Follow up from</td>
</tr>
</tbody>
</table>
**APPENDIX 3**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event Description</th>
<th>Type</th>
<th>Organizers</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 21</td>
<td>LvZ-LU</td>
<td>Discussion with the Knowledge Platform Identity of the Dutch government.</td>
<td>Panel discussion</td>
<td>Government NL</td>
<td>Invited to advise on communication strategy</td>
</tr>
<tr>
<td>May 22</td>
<td>LvZ-LU</td>
<td>Discussion with the Open Data Platform of the Dutch government about public attitudes to open data.</td>
<td>Panel discussion</td>
<td>Government NL</td>
<td>Visibility to representatives of national and local government</td>
</tr>
<tr>
<td>June</td>
<td>LvZ-LU</td>
<td>Meeting with the Science and Technology Committee of the House of Commons inquiry about public attitudes to Social Media Data and Real Time Analytics.</td>
<td>Oral evidence</td>
<td>Parliament UK</td>
<td>Taken up in committee report</td>
</tr>
<tr>
<td>June</td>
<td>ALL</td>
<td>Presenting final outcomes of IMPRINTS with Global Uncertainties Impact Champion Tristram Riley-Smith.</td>
<td>Policy seminar</td>
<td>Government UK</td>
<td>Visibility</td>
</tr>
<tr>
<td>July 3</td>
<td>LvZ-LU</td>
<td>Meeting with the Project Team Communication E-ID scheme about research and communication strategies for the new Dutch scheme.</td>
<td>Advice</td>
<td>Government NL</td>
<td>Changing communication strategy</td>
</tr>
</tbody>
</table>
## IMPACT ON INDUSTRY STAKEHOLDERS

<table>
<thead>
<tr>
<th>YEAR</th>
<th>DATE</th>
<th>WHO</th>
<th>CONTENT</th>
<th>ACTIVITY</th>
<th>TARGET</th>
<th>EFFECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>January 27</td>
<td>ALL</td>
<td>Introducing IMPRINTS to stakeholder committee.</td>
<td>Meeting</td>
<td>Stakeholders</td>
<td>Visibility to bespoke group of stakeholders</td>
</tr>
<tr>
<td></td>
<td>September 12</td>
<td>ALL</td>
<td>Stakeholder meeting discussing progress.</td>
<td>Meeting</td>
<td>Stakeholders</td>
<td>Only one present</td>
</tr>
<tr>
<td></td>
<td>ALL</td>
<td>Nominated for the ID-next innovation award.</td>
<td>Award</td>
<td>European Identity Management Industry</td>
<td>Industry recognition</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>August 27</td>
<td>LvZ-LU</td>
<td>Keynote to Shine Nordics annual ideas conference, about the future of electronic identity.</td>
<td>Oral presentation</td>
<td>Nordic region’s largest film and TV production group</td>
<td>Visibility, ideas generation</td>
</tr>
<tr>
<td></td>
<td>October 23</td>
<td>LvZ-LU</td>
<td>Children’s workshop at Biometrics Annual Conference about identity technologies in film and TV.</td>
<td>Workshop</td>
<td>Children, biometrics industry</td>
<td>Visibility</td>
</tr>
</tbody>
</table>
## OUTREACH ACTIVITIES

<table>
<thead>
<tr>
<th>YEAR</th>
<th>DATE</th>
<th>WHO</th>
<th>CONTENT</th>
<th>ACTIVITY</th>
<th>TARGET</th>
<th>EFFECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>March 22</td>
<td>LvZ-LU</td>
<td>Identity collapse, artist workshop with Heath Bunting.</td>
<td>One day outdoor exercise</td>
<td>Student body of LU</td>
<td>About 15 participants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GT-LU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LT-NU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July</td>
<td></td>
<td>GT-LU</td>
<td>Editing Grant Shapps’ a part of 'A State of Un-Play'.</td>
<td>Performance</td>
<td>Bucharest Art Festival</td>
<td></td>
</tr>
<tr>
<td></td>
<td>September</td>
<td>ALL</td>
<td>British Science Festival Newcastle.</td>
<td>Research Kiosk</td>
<td>General public</td>
<td>About 100 visitors</td>
</tr>
<tr>
<td></td>
<td>November</td>
<td>SW-DU</td>
<td>Dundee Science Festival.</td>
<td>Research Kiosk</td>
<td>General Dundee Public</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LGF-DU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EP-EX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>December 3</td>
<td>SW/DU</td>
<td>Public lecture about digital lives and digital identity.</td>
<td>Public lecture</td>
<td>McManus Gallery, Dundee</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>January 29</td>
<td>SW-DU</td>
<td>How to make a new identity, artist workshop with Heath Bunting.</td>
<td>One day workshop</td>
<td>VRC/CenterSpace, Dundee</td>
<td>About 20 participants</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LGF-DU</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 11</td>
<td>LvZ-LU</td>
<td>Live talkshow in Rotterdam City Theatre about IMPRINTS Research, for screening as well on YouTube.</td>
<td>Interview</td>
<td>General Public</td>
<td>About 100 audience</td>
<td></td>
</tr>
<tr>
<td>March 14</td>
<td>GT-LU</td>
<td>Being A.N. Other, artist workshop by Simon Farid.</td>
<td>Afternoon workshop</td>
<td>Wander Arts Group, The Hague</td>
<td>About 10 participants</td>
<td></td>
</tr>
<tr>
<td>June 26</td>
<td>GT-LU</td>
<td>Ever wanted to be someone else? Artist workshop by Simon Farid.</td>
<td>One day workshop</td>
<td>ISIS Arts, Newcastle</td>
<td>About 15 participants</td>
<td></td>
</tr>
</tbody>
</table>
## Media Attention

<table>
<thead>
<tr>
<th>YEAR</th>
<th>DATE</th>
<th>WHO</th>
<th>Title</th>
<th>Type</th>
<th>Medium</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>June 20</td>
<td>LU</td>
<td>Universities in UK’s best ideas list.</td>
<td>News item</td>
<td>Leicester Mercury</td>
<td>Regional readership</td>
</tr>
<tr>
<td></td>
<td>October 4</td>
<td>LU</td>
<td>Loughborough University to lead international identity management study.</td>
<td>Press release</td>
<td>Targeted News Service</td>
<td>Other media I guess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DU</td>
<td>Dundee to take part in international identity management study.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Source</td>
<td>Type</td>
<td>Format</td>
<td>Details</td>
<td>Authorship</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------</td>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------------------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td>October</td>
<td>ALL</td>
<td>...International Identity Management study.</td>
<td>Discussion thread about the token of the beast</td>
<td>Worthy Christian Forums</td>
<td></td>
<td></td>
</tr>
<tr>
<td>October</td>
<td>ALL</td>
<td>Moving closer to total identity management.</td>
<td>Discussion thread based on press release</td>
<td>Stormfront, <a href="https://www.stormfront.org/forum/t837231/">https://www.stormfront.org/forum/t837231/</a></td>
<td>Neo Nazis</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Source</td>
<td>Description</td>
<td>Type</td>
<td>URL</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------</td>
<td>------------------------------</td>
<td></td>
</tr>
<tr>
<td>May June</td>
<td>SW-DU</td>
<td>Interview with Sandra about wearable ID Technologies.</td>
<td>Interview</td>
<td>Wearable Technologies, <a href="http://www.wearable-technologies.com/2012/05/wearables-for-identity-management/">http://www.wearable-technologies.com/2012/05/wearables-for-identity-management/</a></td>
<td>Leading blog for over 3000 wearable tech companies</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Category</td>
<td>Title</td>
<td>Source</td>
<td>Readership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>January 14</td>
<td>LvZ-LU</td>
<td>Electronisch ID moet mooier en leuker (Electronic ID needs to be more beautiful and more fun).</td>
<td>Interview with LvZ AutomatiseringsGids <a href="http://www.automatizingids.nl/achtergrond/2014/01/leesbet-van-zoonen-elektronisch-id-moet-mooier-en-leuker">link</a></td>
<td>IT professionals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>June 23</td>
<td>LvZ-LU</td>
<td>SOCIAL MEDIA DATA AND REAL TIME ANALYTICS SKILLS AND INFRASTRUCTURE.</td>
<td>Announcement of participation LvZ in committee hearing States News Service</td>
<td>Press release UK government News</td>
<td></td>
<td></td>
</tr>
<tr>
<td>June 24</td>
<td>LvZ-LU</td>
<td>Big Brother Watch gives evidence to parliament.</td>
<td>Big Brother Watch. <a href="http://www.bigbrotherwatch.org.uk/home/2014/06/big-brother-watch-gives-evidence-parliament.html">link</a></td>
<td>Privacy activists</td>
<td></td>
<td></td>
</tr>
<tr>
<td>June 25</td>
<td>LvZ-LU</td>
<td>Social media data and real time analytics skills and infrastructure.</td>
<td>European Union News</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IMPRINTS (Identity Management – Public Responses to Identity Technologies and Services) is a comparative and multidisciplinary research project conducted by four universities: Loughborough, Dundee, Northumbria and Essex.

It examines the influences on UK and US publics to engage and/or disengage with identity management practices, services and technologies of the future. These involve, among others, new forms of biometric authentication; innovative ‘smart’ tokens like ID or customer cards, jewellery, garment, or further enhanced smart phones. These technologies have become subject to paradoxical processes of acceptance and rejection, with members of the public warmly embracing the one and fiercely rejecting the other, policy development and user-centric applications.

The research took place between 2011 and 2014, and was funded by the Engineering and Physical Sciences Research Council of the UK. Project no: EP/J005037/1

www.imprintsfutures.org

Find us on:
www.facebook.com/imprintsfutures
twitter @imprintsfutures
pinterest.com/imprintsfutures/