An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies

PAM BRIGGS, Northumbria University
LISA THOMAS, Northumbria University

Identity technologies constitute one of the fastest growing areas for research and development, driven by both commercial and administrative imperatives. Crucially, they constitute the means by which we include or exclude individuals and groups in terms of access to goods, services or information- yet few developments in this space embrace an inclusive or value sensitive design philosophy. We describe a rigorous exercise in which we source scenarios that capture new research in the identity space and use these as probes in an inclusive design process. Workshops were held with 6 marginalized community groups: young people, older adults, refugees, black minority ethnic [BME] women, people with disabilities, and mental health service users. Our findings echo Herzberg's two-factor theory in that we are able to identify a set of relatively common values around sources of potential dissatisfaction [hygiene factors] as well as a set of motivators that are differentially valued across communities.

Categories and Subject Descriptors: **J.4 [Social and Behavioral Sciences]**: Psychology

General Terms: Design, Human Factors

Additional Key Words and Phrases: Value Sensitive Design, Inclusive design, Identity Management, Hygiene Factors, Marginalized Communities

ACM Reference Format:

1. INTRODUCTION

Identity technologies, broadly defined, are those technologies that allow us to display information about ourselves. They encompass those systems used to foster individual self-expression and personal archiving, as well as gatekeeping and authentication technologies which are used to define and enforce citizenship at various levels – fostering both access and inclusion. The design of such technologies – whether they are constructed for social exchange or for authentication purposes – says something profound about who we want to be, both as individuals and as a society. For this reason, it is curious that so little work in the identity space has adopted an inclusive design approach so that identity technologies can fully serve all sectors of society. The principles of inclusive design are simple: give sensitive consideration to all potential users of a technology early in the design phase [Newell and Gregor 2000]. This includes users with disabilities as well as those marginalized by virtue of their age, ethnic, social, religious or political background. The arguments in favor of

This work is supported by the Engineering and Physical Sciences Research Council, grant EP/J005037/1.

Author's address: PaCT Lab, Northumbria University, Psychology Department
Northumberland Road, Newcastle upon Tyne, NE1 8ST, UK.

DOI:http://dx.doi.org/10.1145/0000000.0000000

inclusive design are not simply about equity and ethics, but are more profoundly about embracing a value sensitive process that can yield products and technologies that give more delight and functionality to everyone.

In this paper we view identity technologies through an inclusive design lens in order to create a roadmap for future research and design. There were two phases to our research: firstly, we mapped out the future design space for identity technologies, using a rigorous sampling methodology that yielded a library of futuristic scenarios and artefacts, representing widely different technologies and practices [e.g. biometrics, implants, social media] across a range of contexts [e.g. border control, access to health-care, lifelogging]. Secondly, we used these scenarios and artefacts as probes and provocations in a series of workshops with marginalized communities including young people not in education, employment or training [NEETS], older adults, refugees, black minority ethnic [BME] women, people with disabilities, and mental health service users. Our goal was to identify the costs and benefits of different design decisions across many communities in order to signpost those development areas most likely to be broadly, if not universally, acceptable.

2. BACKGROUND RESEARCH

The technological mediation of identity embraces key issues of citizenship, privacy and self-expression. Large-scale national identity management projects are underway both in the UK, where an identity card program rejected by the British public is being replaced by a federated identity assurance system [see gov.uk], and in India where the government is rolling out a country-wide system for biometric identification [Singh 2011]. Such initiatives sit alongside commercial developments that seek to support users in their everyday management of finance, health and wellbeing or, more creatively, in their presentation and curation of self. Although such disparate identity technologies are seldom considered within one framework, there is a growing recognition that a more unified approach to the computational mediation of identity would be useful – and further, that such an approach should be not only citizen-centric but also inclusive in recognizing the diverse citizen needs that a good identity system should address.

A recent UK Government report on the future of identity highlighted three relevant trends: [i] increasing hyper-connectivity, where mobile penetration acts to reduce meaningful differentiation between online and offline groups; [ii] increasing social plurality, based in part by the demographic shifts of an ageing population, but also reflecting technology's ability to support dispersed, virtual communities; and [iii] blurring of public and private identities, reflecting a new willingness to curate and share personal information via social media [Foresight Future Identities 2013]. The authors conclude:

> "Citizens will increasingly be characterized as hyper-connected individuals who make choices which reflect their identities. Simple categorizations based on 'traditional' notions of identities are likely to become less meaningful in the digital age as it gathers pace over the next decade".

This sets a political or policy context to the current paper, underpinned by the range of different national and international agencies that have pointed to identity management as one of the main private and public challenges of the future [Camenisch et al. 2011; Gartner 2012]. However, there is also a commercial context which is reflected in the success of those businesses that support the explicit

promotion of identity by an individual citizen [via social media platforms] and also in those businesses that support the implicit harvesting of identity in the form of a commercially valuable profile of individual consumer preferences and habits [social media providers, advertising services and major retailers].

As a final note, we should remember that there are social and creative contexts to the technological mediation of identity. Lindtner et al. [2011] has noted, for example, that the digital exchange of identity information is often part of a creative process that allows for the individual expression of ideas, but that also aids in the development of trusted relationships and in the creation of a strong sense of collective belonging. Of course technological support for the *performance* of identity [Goffman 1959] has been greatly enhanced by the creation of social media vehicles allowing the expression of different versions of self, as noted by Lindley et al. [2013].

2.1 A comprehensive approach to identity

Identity is not an easy construct to work with. Long gone is the sense that identity is a label ascribed to an individual reflecting a given name and/or position in society. Instead, we can agree that identity is understood in different ways and that it comprises components that are intrinsic or inherited [e.g. race, gender, eye-color], ascribed to an individual [e.g. name, social security number, system identifier] or elective components that an individual chooses in the presentation of self [e.g. Twitter names, selected photographs and characteristic personal displays such as dress or communication style]. These elective components can help us establish and differentiate among multiple identities [in simple terms: we may dress differently for work than for play, just as we may use 'LinkedIn' as a vehicle for work displays and Facebook for family and friends]. It is interesting in this context to note that, at the heart of academic writing about identity, there lies a tension between striving for identity coherence [Giddens 1991] and striving to create a range of identities that are performed in context [Goffman 1959].

Together, the intrinsic, ascribed and elective elements of identity form the raw materials for designers of identity technologies. However, until recently they have been subject to very different research and design traditions. Intrinsic or ascribed elements have typically been the focus for computer scientists and biometrics experts working within a hard security and authentication tradition. In contrast, elective identity displays have more frequently been discussed within a sociological or psychological framework. Examples here would include work on technology and self [Turkle 2012] and the social displays of teenagers [boyd & Marwick 2011].

2.2 Technology mediated identity

These research traditions may be distinctive, but technological developments have imposed a certain unifying principle across the identity space. Put simply, computer mediated identity work of whatever flavor is increasingly practiced on one common device. A smartphone, for example, gives a user access to government, retail or financial services - operations that typically require hard authentication techniques - sometimes including a biometric assessment delivered by the same platform. Alongside this, the smartphone also provides the vehicle for social media applications that foster various forms of identity play – via Facebook, twitter, Pinterest etc. We are now weaving together these different identity elements in unprecedented ways, which means that we face new opportunities [e.g. in federated identity management] but also new threats [predominantly to personal privacy] with the commodification of our own personal histories and preferences.

One of the implications of using machines to do our identity work is that the 'social construction' of identity becomes a public record [e.g. Briggs 2013]. Increasingly, we leave a trail of data artefacts that can be used by others, which means that, in two very real senses, we lose control of our online selves: firstly, we may no longer be the primary creator of our own online identity as others in our social or commercial sphere will do much of the tagging, profiling or curating themselves. Secondly, it follows that we may no longer be able to remove or edit these digital selves, indeed, we may not even be aware of their existence – an issue at the heart of new EU developments around 'the right to be forgotten' - a Data Protection Regulation that has been developed by the EU justice commissioner's office primarily in response to complaints about the way social media companies retain and handle information [House of Lords report 2014].

In summary, then, whether using a handheld device as a biometric platform, or using a home computer to upload holiday photographs, the identity work that these machines do for us allows us to do three important things: shape our public image, gain access to goods and services, and make a cultural contribution. Such basic activities are fundamental to members of a society – and so it can be worrying that R&D reports in this space seldom reflect new participatory design practices that give prominence to both inclusive and value sensitive design.

2.3 Design Approaches

Two user-centered design practices have informed our own approach to the study of identity technologies. The first - inclusive design – takes the premise that the very best technological developments emerge from a design practice in which the most diverse segments of society are considered, asserting that designing for population extremes can bring benefits for everyone. Part of the underlying rationale for this is the recognition that any one of us can experience the disabling effect of certain types of context or condition. Newell [1995] argues that we can draw a parallel between ordinary people operating in an extraordinary environment and between extraordinary people operating in an ordinary environment. To take an example: if the ambient noise in a room is extremely loud [extraordinary], our [ordinary] ability to hear a phone ringing may effectively be compromised and so our user experience at that point is not dissimilar to that of an individual with a recognized hearing impairment [extraordinary] operating under moderate [ordinary] ambient noise conditions. Thus the goal of inclusive design is the creation of systems that are genuinely usable across all contexts and individuals and this can be achieved by giving explicit consideration to marginalized users or those who experience a range of usability challenges. In the current marketplace Oxo's Good Grips kitchen tools have been cited as a good example of a product where the design brief was shaped around a challenged population [arthritic customers] but where the design solution was considered universally excellent [see McAdams and Kostovich 2011, for a recent discussion]. Newell and Gregor [1997] cite a range of interesting early examples of such inclusive design and include a discussion of the typewriter, a tool which was originally conceived as a writing solution for the blind.

Note that inclusive design could be seen as the British precursor to the growth of 'universal design' [Goodman et al. 2006; Lazar 2007; Shneiderman 2000; Vanderheiden 2000] which also had the premise that design should serve the widest possible sample of the population. However, inclusive design has become more strongly associated with the notion that designing for extremes can produce superior as opposed to satisficing solutions.

The second user-centered design practice – value sensitive design [VSD] – emerged from a heightened awareness of the ethical implications of technological design towards the end of the last century [Friedman and Kahn 1992]. At the heart of this debate was recognition that two values, user autonomy and freedom from bias, were often overlooked in the design process. For Friedman [1996] and Nissenbaum [2010], too many users were made uncomfortable by design defaults that forced the adoption of particular processes and failed to allow them to develop their own work practices [user autonomy]. Added to this was recognition that many computer systems showed systematic bias in unfairly discriminating against certain groups of individuals in favor of others. These two concerns [captured in Friedman 1996] led to the development of VSD and an associated philosophy that helps users challenge new technologies in terms of 'what they think of as important in life' [Friedman et al. 2006; Nathan et al. 2008].

This emphasis is important in the identity technology space, as considerations of individual, corporate or societal good are not always in synchrony. Dystopian variants of the 'big brother' story are frequently premised upon a state roll-out of surveillance systems that offer security assurances to the individual whilst leveraging unprecedented state or corporate access to that individual's data. Recent debate around the Snowdon release of NSA and PRISM surveillance practices have provided a public demonstration that such dystopian practices are not constrained to fiction. This is the design space for identity technologies and so participatory practices must allow users a voice to critique design in terms of fundamental human rights and values as well as individual needs and wants. VSD makes some grand claims in terms of representing societal values – and indeed, critics have said that it overclaims, in the sense that the researcher can assume more authority than may be actually warranted by the scope or rigor of the investigation that generated those claims, or that the claims made for a particular group may not be universal [Alsheikh et al. 2011]. Borning and Muller [2012] suggest that, at its core, VSD should adopt a more humble, pluralistic position – allowing the accommodation of a number of voices and ensuring that the participants themselves are heard in the writing.

In our own study, we have tried to embrace these two practices – inclusive design and VSD – by engaging with a number of marginalized groups around different identity technology futures and by allowing them to discuss values in their own terms. We have therefore tried to act as reporters rather than interpreters – allowing our users to speak for themselves – and we have also tried to be as systematic as possible in the selection of prompts and provocations for discussion, recognizing the underlying problems of researcher bias inherent in qualitative research. Our methods mirror those sometimes found in VSD, involving the presentation of a realistic range of scenarios and prototypes followed by a process of value elicitation that encourages participants to compare and contrast devices but that also allows them the ability to express personal preferences, likes and dislikes. In this, our study is not unlike the investigation of implantable medical devices, as described by Denning et al. [2010] which succeeded in capturing some of the perceived risks associated with design alternatives, but in our study there is also an explicit recognition that we might elicit very different values from different communities [cf Le Dantec et al. 2009]. Our research had two phases involving [i] the sourcing of relevant identity technology scenarios accompanied by good quality mockups, films or other envisionment prompts, which were then used in [ii] a series of workshops with a focus on value elicitation. These are described in more detail below.

3. PHASE I: SCENARIO-SOURCING

We conducted a systematic scenario sourcing exercise designed to generate prompts and provocations for our various communities. These were intended to support a process of envisionment, known to be important in value-elicitation [Satterfield 2001]. Envisionment prompts that employ images can help respondents articulate a broader range of values [Nathan et al. 2008] and in particular, film has been shown to elicit broader, more value-laden contributions from participants in workshops [Briggs et al. 2012; Little et al. 2009; Mancini et al. 2010]. Film has also been shown to be highly effective with older adult user groups [Newell et al. 2006] as it can communicate the essential properties and functions of a new device or system, but can also be used to foreground the experiences of using those technologies, offer alternative experiences or provoke consideration of their wider impact [Mancini et al. 2010; Raijmakers et al. 2005]. The use of high fidelity artefacts and prototypes is also common in participatory design and VSD practice as they can prompt users to identify problems and express their own needs and values [Vines et al. 2012].

We searched for identity management scenarios and artefacts in a wide range of fields, looking especially at scenarios that circulate in the identity management industry, online commerce, government policy, civic activism, popular culture, art and commercial design. In some fields, finding scenarios was relatively easy. The biometrics industry, for instance, has a well-functioning platform that provides the latest news and enables networking, and there are comprehensive databases for news media and popular culture. Civic activism and arts and design are more unruly fields, however, that needed more extensive methods to search for scenarios. In addition, while identity management is a common concept in the industry, it works poorly as a database search term. Thus a pilot search in the Nexis newspaper data base, using "identity management" as the only search term for all UK broadsheets [Daily Telegraph, Guardian, Independent, Observer, Times] of the last ten years, delivered only 92 articles, five of which concerned the management of corporate identity. We therefore decided to employ a fuzzy search strategy, using a wide variety of search terms associated with identity management and stopping the search at saturation, i.e. when no new scenarios emerged.

For each scenario we asked: [i] what kind of identity management technologies are concerned and which innovations are presented?; [ii] which actors and stakeholders are included and in which roles; [iii] what kind of identity interaction is presented [social interaction, security, access, transaction, etcetera]; [iv] what is the social context in which identity management is presented [health, citizenship, politics, education]; and [v] what risks and opportunities are suggested within the scenario?

In total, we sourced over 100 identity management scenarios, organized by context [organizational, social, individual] and application [body-based, token-based, knowledge-based]. The full complement of scenarios elicited is described elsewhere [VanZoonen et al. 2013], but here we give a structural overview and describe the ways in which specific scenarios were selected for presentation in the current study.

Firstly, we noted three contexts in which people present identity information; [i] an organizational context whereby people claim access to goods or services; [ii] a social context where people share personal data with other individuals, and [iii] an individual [typically domestic] context where people claim ownership of a machine by some kind of personal authentication process. Secondly, we noted that the identity technologies and protocols used to authenticate to these different contexts could be classified into [a] body-based systems that typically require some form of biometric or

implant, [b] token based systems that required some form of access card or object and [c] knowledge-based systems that typically required that the user know some kind of secret authentication code [typically password or PIN]. There were also instances where scenarios could be applied to a number of situations. In these cases we tried to explore variations of a scenario. For example, body-based microchip scenarios could be categorized within a social context [microchips to pay for drinks in a nightclub]; an organizational context [dementia patients using a microchip to communicate with medical facilities]; or an individual context [using a microchip to access your car]. In these cases, we employed all three examples to get a better sense of acceptability for each context.

Whilst there was no systematic checking involved regarding the frequency of sources arising in particular contexts, it did become clear that the policy documents we consulted often described more biometric scenarios, whereas sourcing from the arts and design fields often yielded more science fiction technologies. We describe these contexts in a little more detail below – citing examples of the scenarios or artefacts we selected for presentation to our participants.

3.1 The organizational context

Currently we most commonly gain access to public or commercial goods or services via a token-based authentication system that includes passports, identity cards, customer loyalty cards, patient cards and wristbands. Future scenarios typically add smart RFID technology to such tokens and increasingly design tokens to be wearable in the form of textiles and jewelry. Our scenario-sourcing also showed a strong role for biometrics in this organizational context: people are shown gaining access to government or corporate services using, inter alia, finger, palm and buttock prints as well as iris, face, voice, gait and odor recognition. From our policy papers, we noted that such developments were driven by an expanding industry base, but also noted that this was the area where the strongest public and political concerns for the future had been expressed.

In the current study, we selected organizational scenarios that could illustrate these futures and included airport security based on novel biometrics [odor], organizational access based on face recognition, implants or smart tattoos; the use of smart wearables [badges, jewelry] to gain access to buildings or services and knowledge-based authentication and profiling in commercial services [pizza delivery]. The scenarios were selected based on their frequency of appearance in our scenario-sourcing phase [we wanted to show examples where there was a sense of likelihood of occurring in the future], but also some of the more novel or unusual scenarios [odor recognition, ingested authentication pill] to encourage discussions beyond the realistic.

3.2 The social context

We noted the growth of identity exchange in a social context wherein one individual will share identity information with another in order to facilitate future online engagement. Currently typical in this space are the exchanges taking place in various social media platforms in which a user [having first registered identity credentials with an organization] then presents selective identity data to other individuals or members of the same group. However we noted that future scenarios show other identity technologies populating this space – including smart business cards and smartphone face recognition systems that support identity recognition and exchange or even Google Glass which promised augmented [social] reality. Here too

we found technologies that supported lifelogging or digital curation and legacy practices. For our study, we selected scenarios that supported such digital legacy [including QR codes on gravestones and personal heirlooms], augmented social reality [Google Glass, Recognizr App] and wearables capable of transmitting identity information in a social context [e.g. scarf with personalized QR print]. We also noted a number of future scenarios involving identity theft or catfishing and included examples that reflected this more dystopian vision [e.g. takethislollipop.com].

3.3 The individual context

Finally, there is a largely domestic context in which people, acting in isolation, present identity information to machines. This is already commonplace - many laptops or smartphones are secured through a biometric authenticator, most often fingerprint or iris scan and keystroke patterns offer a new means of behavioral biometric that can be used for personal authentication on PCs and laptops. There were a number of scenarios in this space that were derived from new work around the Internet of Things and a variety of 'smart home' technologies, but we selected future scenarios that illustrated the use of implants in the space [e.g. to gain access to a car] or, more radically, the use of smart authentication pills that could turn the whole body into a device that could activate other devices. Other technologies in this personal, domestic space included RFID jewelry and companion or proxy devices that could act as digital guardians [e.g. a biometric daemon- see Briggs & Olivier 2008]. Table I shows the scenarios with context, media used, and participant group workshops they were presented in.

Table I. Scenario information

Context	Scenario	Media	NEETS	Older adults	Refugees	BME women	Disability group	Mental health service users	Intergen.
Organizational	**Pizza delivery video** *A customer calls a pizza shop who store excessive personal details about them*	Video	■	■					
	Odor recognition *Identification of a person by their distinct body odor suggested for identification at airports*	Artefact	■						■
	Biometrics *[face/vein/fingerprint/iris]*	Video, image			■	■			■
	Smart tattoo *A tattoo, visible or invisible, that could be scanned to identify the wearer*	Image			■	■			■
	Microchip [medical] *Implant of a small chip that could be scanned by medical staff to identify vulnerable patients*	Video		■					■
	PsychicID card *A physical card which can identify you in any situation. It only reveals information when scanned by a legitimate entity*	Prototype	■	■		■		■	■
Social	**Recognizr application** *An app. which scans the faces of people near you, and displays information about them on a mobile*	Video		■				■	

	device- the scanned person dictates what information to reveal								
	Google Glass *Official promotional video showing a man using the device on his way to meet friends and utilizing the device's features/parody video showing the wearer being interrupted by adverts, badly placed notifications, bumping into objects in the real world*	Video							
	QR artefacts *Objects imprinted with QR codes being used for identification e.g. T-shirts, scarves*	Prototype							
	QR gravestone *QR code tokens placed on gravestones which link to remembrance websites constructed by family members of the deceased*	Video							
	Lifelogging/quantified self *The example of Gordon Bell, recording all aspects of life; also reference to quantified objects- wearables to monitor self*	Video							
	Take this Lollipop *A social media app. that uses your Facebook content to build a personalized video depicting a stalker viewing your account*	Video							
	Microchip [socializing] *A nightclub in Rotterdam microchips it's patrons to pay for door entry and drinks*	Video							
Individual	**Biometric daemon** *A device imprinted with the fixed biometric properties of its owner- it acts as an electronic pet which needs nurturing and dies when separated from its owner*	Video							
	Authentication pill *A pill with a chip inside it; when you swallow the pill it creates a signal inside your body. The signal enables you to authenticate with phones, computers, cars*	Discussion							
	Microchip [personal access] *The example of Amaal Graafstra, a man who implanted himself with a microchip to gain access to his car, computer etc.*	Video							
	Smart wearables [jewelry, watch] *Artefacts that are implanted with an RFID chip which communicate with services*	Artefact							
	Draw a Secret *Prototype software used instead of a password to enable access to mobile phones is more secure. A picture is drawn on the phone- the user has to pick the right drawing to prove they are the owner.*	Task							
	Driverless car *The example of the Google car, which can be driverless- includes issues of data collection, continual monitoring*	Video							

4. PHASE II: VALUE ELICITATION

4.1 Participants

Our inclusive design approach demanded that we consider the needs and concerns of marginalized populations. We recruited from six different communities, with representation from young people not in education, employment or training [NEETS], older adults, refugees, black minority ethnic [BME] women, people with

disabilities, and mental health service users. Twelve workshops were conducted with a total of 91 participants. Eleven of the workshops were held with individual community groups. This method was chosen to allow the groups to feel at ease. Participants from the BME women's group and refugee groups in particular, felt apprehensive, and were more comfortable working with people from their existing network. The twelfth workshop brought together the NEETS and older adults in order to encourage intergenerational debate- these two groups were more at ease with people they did not know. Details of participants are given in Table II.

Table II. Participant information

	n	Male	Female	Mean age & S.D	Age
NEETS	9	5	4	19 [3.8]	14-24
Older adults	18	6	12	68 [3.7]	62-76
Refugees	12	3	9	39 [9.6]	28-56
BME women	6	0	6	40 [7.9]	29-48
Disability group	7	4	3	47 [9.6]	33-59
Mental health service users	13	9	4	49 [8.8]	36-65
Intergenerational group	26	11	15	Younger: 20 [3.3] Older: 69 [6.4]	16-25 56-76

4.2 Procedure

The eleven community workshops involved between four and seven participants, and lasted around 2 hours. One facilitator working on the project managed and recorded discussion; sessions were guided by a semi-structured interview schedule, designed to present scenarios to participants in turn. Each technology was presented via a short video, a physical artefact [e.g. a working prototype], a written scenario to exemplify use, or a collection of photographs. Approximately four scenarios were presented in each workshop. Each workshop group had the opportunity to experience a range of scenarios, but the materials used to describe each scenario remained constant. We aimed to use scenarios which covered each possibility in the framework that emerged from our scenario-sourcing phase [see VanZoonen et al. 2013], identifying contexts [organizational, social, individual] and a means of expressing identity [body-based, token-based, knowledge-based]. From this framework, we chose scenarios for each workshop to give participants a broad range of issues to discuss. Thus, whilst scenarios presented in each workshop may not have direct links to each other, they came from different categories of context or use. Some scenarios we considered more pertinent to particular groups; for example, microchips for Alzheimer's patients was a scenario presented to our older adults- where possible we picked scenarios according to likely exposure to, or experience of it for our workshop group.

The kind of media adopted was guided by the initial scenario-sourcing exercise- some scenarios were originally portrayed in a film [for example, Living Memorial's QR gravestone promotional video] so we showed the original film to participants. Other scenarios, such as biometric odor recognition, were found in scientific reports- so we used props to encourage debate. Each scenario presented was preceded by a brief verbal description [given by the facilitator] of the scenario, and how it might be used in everyday life. For example, the psychicID card was described as being used in a doctor's surgery to present to the receptionist, but also as proof of age when buying alcohol at a supermarket. Participants were asked to talk freely about their

perceptions of the scenarios presented to them, and to consider applications beyond those given. The facilitator refrained from presenting the scenario in a positive or negative light, but encouraged participants to think of positive/negative use cases. Prompt questions such as *'Do you think this technology is acceptable?'* or '*Who would you allow to see this information?'* were used to keep participants engaged with the task.

During the intergenerational workshop participants were divided into 4 tables with a mixture of the NEETS and older adults [twenty-six participants in total]. Each table had a facilitator, familiar with the project, who directed conversation and encouraged participants to think about a number of the scenarios identified in Phase I, as well as encouraging more general future-gazing conversations. The intergenerational workshop lasted around 5 hours. This longer session provided the opportunity for participants to discuss a broader range of topics, but also allowed them to move around the tables and talk about scenarios with different people, thus considering new perspectives.

4.3 Thematic analysis

The audio recordings were transcribed and sentence-by-sentence thematic analysis was employed using NVivo qualitative software. The analysis process followed stages recommended specifically for thematic analysis, namely: [i] familiarization with data [reading and re-reading transcripts]; [ii] generating initial codes [constant comparison between data]; [iii] searching for themes [identified when patterns and repetition emerged in the data]; [iv] reviewing themes [checking themes against extracts and overall data set]; and finally, [v] explicit naming of themes [Braun and Clarke 2006]. We did find that certain participant extracts could be categorized into more than one theme - in this instance we placed quotes into the theme they best represented. Reliability coding was conducted between two members of the research project team- initially one researcher began coding the data, and identified potential themes to explore. The second researcher was then asked to review these themes independently. This was achieved by sifting through printed data excerpts. Subsequently both researchers engaged in a number of review sessions to refine themes and come to agreement on their exact labelling. This was conducted over a period of about a month, and ceased when all potential themes had been identified and researchers were in agreement. Importantly, the categories and overarching theoretical framework [see below] identified in data were derived after thematic analysis had taken place. Conforming to Braun and Clarke's 'theoretically flexible' approach to analysis, preconceived ideas about possible categories or patterns that might emerge were suspended.

5. RESULTS

As a result of this thematic analysis, we were initially able to identify a set of themes or values that seemed common across communities. This, at first glance, would seem to echo an original interpretation of the VSD work that suggests a set of recognized universal values can underpin the design of systems-for-all [Friedman et al. 2006], which is in itself a view that is highly contested [Borning and Muller 2012]. Note that we are not claiming that all of the values we have identified in this work are universal – indeed, we were able to identify several strongly held beliefs that were tied to specific communities. For example, our BME women were very clear to dismiss any form of identity management involving tattooing, implants and/or piercing as abhorrent - such practices violated religious beliefs that the body could

not be subject to such forms of mutilation. However, we were able to identify a set of values common to all of our communities that were deemed *necessary but not sufficient* for uptake and acceptance of any new identity system. We have called these hygiene factors, as they reflect Herzberg's [1966] argument that there exist a set of conditions that are a necessary pre-requisite for engagement, but that don't in themselves generate satisfaction.

Let us consider Herzberg's thesis in more detail as we draw on it more extensively below. He conducted his original studies in the workplace, where he noted that those factors that led to employee dissatisfaction were of a very different nature to those factors that led to employee satisfaction. The first set, termed 'hygiene factors', included company administrative and supervisory practices, physical working conditions, job security and salary. They had to be right for an employee to wish to continue working for a particular firm, but weren't in themselves sufficient to produce improved performance. The second set, termed 'motivators' tended to be more sensitive to individual employee abilities and needs, reflecting the setting of appropriate goals, the autonomy required to achieve those goals and the sense of achievement that resulted from fulfilling those goals.

Within design research, Herzberg's theory has been taken up by Kano et al. [1996] in terms of two forms of design quality that address either basic needs [must haves] or that address excitement needs [delight]. In HCI, hygiene factors have sometimes been associated with requirements around security and privacy – offering little in the way of user satisfaction, but providing a robust and reliable design [Loser and Degeling 2014], whilst motivating factors have been associated with systems that 'add worth' either individually or collectively [Cockton 2006; van Biljon et al. 2008].

Returning to our own study, hygiene factors can therefore be seen in terms of the fundamental prerequisites for engagement with identity technologies. Things that simply need to be right before users will accept a particular system. We have identified three clusters of hygiene factors here that were supported by all of our participant groups: [i] legitimacy – there should be some reasonable justification for the implementation of the overall system and all forms of data access, collection and storage must be defensible [ii] competence - identity systems should be usable, trusted, reliable and secure, [iii] choice – the systems should allow users some degree of flexibility or personal autonomy in determining level of engagement.

This last is perhaps the most controversial – as there are a number of systems that demand a submissive or compliant response from the user in the sense that they must present a set of identity credentials before gaining access through a recognized physical or virtual gateway; but even here, choice can be important. Consider, for example, new forms of airport security or border control via biometric screening. In both of these cases it is possible to identify individuals [e.g. with various forms of disability] or circumstances [e.g. a mother taking care of a young family] in which some alternative, more sensitive means of screening entry are preferable.

In the section below, we discuss these three hygiene clusters in more detail, before turning to a discussion of the different kinds of motivators that exist in the identity space. Again, we are using Herzberg's term to describe those factors that might bring added value to individuals and/or communities. Note that we found significantly less commonality between our communities when discussing motivators and so, in this section, we try to tease apart some of the distinctive ways in which different communities may be drawn to certain identity technologies.

5.1 Hygiene factors

In Herzberg's original thesis, hygiene factors defined the environment or context within which work occurs, as a result of a desire to avoid unpleasantness. Hygiene factors included salary, job security, working conditions and supervision, and were deemed the major environmental aspects of work. Also termed 'dissatisfiers', these have to be accounted for before 'satisfiers', or motivators, can be considered. Three hygiene clusters were identified in our participant interviews, reflecting significant public concerns around the design and implementation of identity technologies.

5.1.1 Legitimacy

Legitimacy refers here to the sense that there was some clear underlying justification for the structure, form and implementation of new identity systems. The term legitimacy is used in a number of reports and articles which comment on technological evaluation [see Eckfeldt 2005]. The idea of proportionality is relevant here too, stating that: 'personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In addition, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed' [Zorkadis & Donos 2004]. Our participants expressed concerns about both the policies and practices underpinning identity technologies, asking 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. These issues are expressed in the participants own terms as follows:

Data segregation

People felt strongly that different types of data should be stored and accessed independently, with strict data-specific access controls. Such beliefs reflected a sense of unease around the big data revolution and the potential for privacy violation on a large scale. There was a strong sense, from our participants, that the strict segregation of identity data would help ameliorate some of the most pressing 'Big Brother' concerns around surveillance:

> "If your bank is in charge of that, the NHS is in charge of that, and so on and so forth. The government in charge of the government bit… So that independent sources can't get all your details" [NEET, female, PsychicID card].

> "I would only allow a trader to have information about my trade with them and not with any other person. So if I go online to Tesco and it says do you want to have a look at your favorites then that's fine, but if I go to Sainsbury's I don't want them to see what I buy at Tesco" [older adult, male, pizza delivery video].

> "I was thinking that if you had a card which had four separate bits on it, maybe more – there is one for bank details, there is one for health and then say if you are in hospital and they scan it, it only picks up the ID for the health stuff, or if you're in the bank only picks up the bank ID and stuff like that" [NEET, male, PsychicID card].

Here our participants clearly expressed a desire for segregated access to their personal information. This issue was raised in particular when a prototype

'PsychicID card' [Birch 2009] was presented to them. This card ensures only context-relevant information displays on the screen when presented to a legitimate entity. The PsychicID card was welcomed as a step towards improving data segregation; however participants still believed that information being stored on one card remained problematic.

Data integrity

Participants expressed concerns around the malleability of data once it was in the public arena. These concerns took two forms – firstly, they recognized that certain forms of identity information [age, address, qualifications] would require updating, but weren't sure whether the technologies under discussion would keep such information current and valid:

> "We were thinking that maybe if it was something that we could update ourselves, maybe update it on the computer to say we have got this condition or even if you did it with the doctor at the time- plug it in and all the data is updated together" [NEET, male, PsychicID card].

> "You take that information once it's on there, say you changed your address or something, would you be able to change it without having to take the chip out every time?" [older adult, male, microchip (socializing)].

However, participants were also concerned that information created by them could be corrupted by others - with notions of trolling, hacking and identity theft presented as areas of particular concern:

> "What worries me is the fact that people could come along and add to it, because you see for yourself what Facebook is like" [older adult, female, QR gravestone].

> "And who is going to put all this information in the chip, is it me or somebody else? … Me! I would want to do it myself" [BME woman, PsychicID card].

Data access

A very important element arising from our discussions of identity technologies and systems concerned the problem of unauthorized or unjustifiable access to personal data. Participants were troubled by the thought that there might be poor control over who was able to access or manage their identity data:

> "Who gets access to that data? Does the state get access to it? Is it on one universal database? Is that managed by a government agency or a private contractor? Would the private contractor be able to sell your information either legally or illegally?" [mental health service user, male, PsychicID card].

> "If she is a pizza lady she should know what my address is, what my phone number is, and what I have ordered in the past. And that's it. And basically it should be up to me to say to these people this is the level of data which I will allow them" [older adult, female, pizza delivery video].

> "If I phoned a taxi company then they know where I am, so you don't have to tell them. But I don't want them to know what waist size I have or my cholesterol level, so it's a question of appropriateness. But if I phoned the doctor I might want

them to have instant access to my records. Say I am feeling faint, and they say oh you have a problem with your heart so we will get an ambulance to you straight away. So it's a question of an appropriate level of data for whoever it is you are calling" [older adult, male, pizza delivery video].

Our three insights around legitimacy [data segregation, data integrity and data access] may seem highly technical constructs, but there is a strong social and civic message here around privacy. The themes resonate very strongly with Nissenbaum's [2010] ideas of understanding privacy in terms of contextual integrity. Nissenbaum argues that while there are no universal privacy norms, various social norms exist to govern the kinds of information flow that seem appropriate to different contexts. In a health context, for example, an appropriate 'norm' would be that your doctor has access to your medical records, whereas a teacher having access to those same medical records would constitute a privacy violation i.e. would not show contextual integrity. Note that such privacy issues are reflected in other adaptations of Herzberg's work to HCI, where, for example, concerns around the privacy and security of a particular website [CNN.com] were labeled as 'hygiene' factors in a study of website design and evaluation [Zhang and von Dran 2000].

5.1.2 Competence

There were common concerns around whether new identity technologies and systems would be designed competently – i.e. such that they could be trusted to operate reliably, effectively, securely and safely. Such concerns were applied to people as well as to the technologies themselves.

Trust

Incidents demonstrating some form of incompetence were generally associated with a lack of trust in the powers of government or large businesses to maintain secure records. Often these opinions reflected personal experience or larger scale media reports of security breaches:

"I don't even trust my bank with my bank details to be honest with you because Nationwide, they lost how many peoples' bank details?" [NEET, male, smart wearables].

"I do not know who to trust. It is people working for the company. Sometimes the company looks good but people who are doing the attacks are selling stuff out, that is what we find. Everywhere, you know, selling information" [refugee, male, smart wearables].

Trust in computer-mediated exchange not only involves judgments of competence but also judgments about the perceived integrity and benevolence of the service provider [e.g. McKnight, Choudhury & Kacmar 2002]. Mistrust is thus a reflection of the consumers' own beliefs about those organizations or agencies likely to misplace or misuse personal information. Consumer trust is important as it remains a highly significant predictor of both uptake and continued use of e-services [Flavián and Guinalíu 2006], yet we find that users rarely trust governments and business organizations to protect their privacy. In a recent study, 91% of US adults felt that consumers had lost control over how personal information is collected and used [Madden 2014] and it is widely recognized that many private companies will share

data for financial gain. In addition, governments have made a strong security case for 'snooping' on personal citizen data. In the summer of 2014, for example, the snooping practices of UK government security service GCHQ were widely discussed in the press and broadcast media and were recognized in a subsequent UK Government publication in terms of a loss of public trust [House of Commons, Science and Technology Committee 2014]. Note, too, that in labeling trust as a 'hygiene' factor, we see some resonance with earlier work on web design that saw impartiality and freedom from bias as key hygiene constructs [Zhang and von Dran 2000].

Reliability

Participants felt that some systems would simply not work, would be unreliable, or become obsolete. Such reliability concerns were particularly prevalent for those technologies, such as biometrics, that carry the promise of seamless authentication, but that have also been associated with public concerns around informed consent [Krlic 2014]:

> "With biometrics we use it at school for our dinner money and the machines aren't that reliable. Say you put your finger on it…, and there is one thousand five hundred people in my school or something. And obviously you have got fingerprint on a fingerprint, and it has happened to me before - it has come up with different people. So essentially you are gaining access to their stuff" [NEET, male, biometrics].

Note that participant opinions came from direct experience with identity technologies [for example teenagers talked of their school's fallible fingerprint lunch payment system which led to the use of pen and paper], others recounted popular science fiction films and programs which document the failings of biometric technology:

> "What happens if it broke as well, nothing would come up. And they would be like "well you are not this person", and you would be like well I am, it's obviously just broke [sic]. Because everything is on the one card, and then you wouldn't be able to go to the bank or to the doctors or anything" [NEET, male, psychicID card].

> "It's so easy to copy someone's fingerprint. All you need is a bit of sticky tape. Some talcum powder. You run it over anything someone has used, go on someone's computer, and you're accessed!" [NEET, male, biometrics].

> "I have always thought retinal scans should be the way forward because fingerprints are too easily copied. If there's a bit of chewing gum… you see it on the movies" [NEET, female, biometrics].

Often, as above, a perceived failure or vulnerability of an identity technology was associated with a risk of identity theft, which is itself interesting, given that most of the research around identity theft shows it as an expert crime, involving sophisticated and highly targeted access to personal information [Vieraitis et al. 2014]. Our participants were certainly aware of the existence of sophisticated attacks [see below], but here we see a strong perceived relationship between an unreliable system and the associated opportunity for abuse.

Security

Most participants anticipated system failures of one kind or another and talked about data loss as though it were inevitable. Such arguments were often tied to the notion of being defenseless against a sophisticated attack, but led to discussion around the different kinds of personal vulnerabilities that the misuse or misappropriation of identity technologies could lead to:

> "People are so clever these days in gaining information illegally. You know, fool proof cards which cannot possibly be stolen are stolen in ten seconds. It's just too dangerous to have everything on there" [older adult, female, PsychicID card].

> "It is about the security. So many fraud things going on the internet, I am scared to even shop internet. If I do something on the internet I try to use my credit card just for internet purposes I just use it for that otherwise I – because I am not comfortable to use my debit card on the internet. Yes so what is the security and how secure this system will be?" [BME woman, psychicID card].

> "My friend does everything online, she buys her groceries, she buys her clothes, she sells her clothes. She's had her identity stolen twice and this is what I don't like about technology" [older adult, female, QR gravestone].

> "It's good having it in a scarf because you can wear it every day, but if you lost it then someone maybe could pass themselves off as you. Put your scarf on and sort of like, identity theft. If you lost it, you've lost everything" [NEET, female, QR artefacts].

Again, we see the concern around identity theft, although in this case accompanied by the recognition that carrying identity tokens of various kinds [cards, wearables] can render the owner vulnerable to physical attack. Such concerns reflect the reality that stolen cards and documents do indeed play a major role in identity theft, although as we noted earlier, increasingly sophisticated online phishing techniques are also employed [Vieraitis et al. 2014].

Safety

A final set of responses concerned the physical risks associated with some of the latest identity technologies. Some participants – particularly those drawn from the older adult and refugee groups – were concerned about the extent to which they were competent to judge the safety of implants and other physically invasive identity and authentication systems:

> "Personally, I don't think I would go for the [micro]chip because I do not know how much the research is. How much research has been done about it, to make sure? I mean, does it harm people?" [refugee, male, microchip (socializing)].

> "This might sound naïve, but could your eyesight be damaged by having these things in your eyes?" [NEET, male, Google Glass].

> "I honestly think there's hidden health things because there is more and more research coming about implements that are held or put into your ear and what those waves do to a few million brain cells each time and I think the culmination of all that research is going to kick back in about twenty years' time when people

> have gross hearing difficulties, get more mental health issues, because of these alien things" [older adult, female, biometrics].
>
> "What might the thing under his skin do to him in the long run? Do they know yet? Won't it cause septicemia or something?" [older adult, male, microchip (personal access)].

Unsurprisingly, physical safety was more likely to be raised in response to those new, untested technologies that were either highly invasive or that were likely to be worn for long periods of time. We see similarities here with patient concerns around implantable medical devices [IMD] where the embodied nature of such devices can be a trigger for anxiety [Denning et al. 2010]. Note that while we might expect to see some cultural differences in terms of what may seem safe or appropriate, particularly in regard to implant technologies [see Michael & Michael 2014], there was a more general anxiety, shared among our participant groups, that radical new technologies might simply hit the market too soon. We should note, too the resonance with Herzberg's original thesis, where health and safety issues were clearly signposted as hygiene factors within the workplace.

5.1.3 Choice

Many scenarios provoked a discussion of personal choice encompassing the extent to which levels of engagement with any particular system may be mandatory, but also addressing mediating variables that might mitigate choice – such as the usability or the cost of the system under discussion. Issues around informed consent and personal autonomy were paramount here.

Opt In

Fundamentally, participants were happy to accept identity management technologies provided they could choose to adopt them if they wished. The thought that some technologies would be compulsory was met with resistance and frustration:

> "I suppose with a lot of things as well is it's important the choice is whether you engage with it, I mean it can be out there and maybe half the people would use it but if you choose not to well that's fine, it's your choice" [older adult, female, QR artefacts].
>
> "As long as it doesn't become law, as long as it's optional. For those that need it and they want to do it then that's fine, but when I don't have a choice then I have a problem with that. I want to have the choice to say okay" [refugee, female, biometrics].

There was also a strong sense that the dangers associated with some kind of 'creeping compulsion' to use the new technologies should be carefully considered. Participants recognized the development of new social norms around technology use, that meant that what might be unacceptable at one time point might become commonplace in another, but they worried about the overall effect on social capital, the expected collective benefits derived from cooperation between individuals and groups. Again, in the tradition of VSD, we see a collective call to protect our future selves and to think about the longer-term:

> "This thing won't just affect individuals; it will affect the whole of society. So even those who don't adopt this technology, their lives will be impacted by it. So there needs to be not just the assessment of 'Oh this will make your life easier', alright it might make my life easier but I'm not interested in just that, I'm interested in how it will impact society as a whole" [mental health service user, male, Google Glass].

> "All the mums are at work now, you go out in the morning, out the front door, into the car, come back, you don't see the neighbors. You can get your groceries online, you don't even need to go to the shops now so all those things, we know it'll change our lives but how will it change them?" [older adult, female].

Diversity & exclusion

Ethical concerns were also raised in relation to the kinds of identity systems that might be imposed upon vulnerable adults who were not able to give informed consent – an issue that led to discussions around population control and social engineering in respect of those with disabilities:

> "The thing with that kind of technology is where do you draw the line with people with disabilities? It's obviously a big thing, with all this technology they're doing now in hospitals, finding cures for different ailments so they can try and get a sort of Aryan community" [older adult, female, microchip (medical)].

> "I think with biometrics, because not everybody is the same, not everybody has hands, because not everyone has eyes, you know, you presumably have to have, there would still have to be options. Maybe you've got a choice, each machine is workable with eyes, fingers, or breath, is that the way it would go in then?" [disability group, male, biometrics].

Exclusion was often seen as an unintended design consequence following the introduction of some new kind of authentication system. Often such issues were raised most passionately in relation to biometrics or other physically modulated systems that carried accessibility or ease-of-use requirements:

> "It needs to be accessible. I can't see you presenting your knee to a door lock!" [older adult, female, microchip (personal access)].

> "The thing is when you've got a fingerprint reader is can you reach it, can you use it physically? The iris readers, you know, the passport ones now they have at passport control, you've got to be standing in the right spot, they move it up to your eye level until it finds your eye level and if you're sat in a wheelchair how does that work? It probably wouldn't" [disability group, male, biometrics].

However, financial cost was also seen as a barrier to engagement – effectively generating further exclusion as not everyone would be able to afford new systems, or be penalized if they lost their expensive equipment:

> "Whatever system you try and put in place, the cost is so phenomenal isn't it, like DNA, every place that you visit would have to be fitted with some machine that could receive this information" [older adult, male, biometrics].

> "How it will be replaced if somebody loses it, how will it be replaced and do we need to pay extra or whatever because I am not going to pay extra money. If I've got a card and I lost it, I ring my bank and they block my card and send me new card. Will that same thing happen with this [micro]chip or this card?" [mental health service user, male, PsychicID card].

> "And then how much would it cost? Am I going to pay, how would this work?" [BME woman, PsychicID card].

5.2 Motivators

In Herzberg's original thesis, motivators were those factors that brought additional value to the workplace and typically reflected the values associated with positive, heightened experience [Herzberg 1966]. These were the 'satisfiers' that came from a sense of performing interesting and important work and led to achievement, recognition, advancement and growth [Herzberg 1987]. Subsequent work in the technology domain suggests that such motivators can act at the inter-personal level [in providing some kind of social or communicative value] but can also act to enhance the interaction between human and machine - where, for example, the hedonic properties of a device or experience become valuable in themselves [van Biljon et al. 2008]. An example here would be the pleasure that might come from a wearable form of identity authentication, such as an attractive bracelet or ring that serves to grant seamless access to a vehicle or home.

Returning to the argument around the universality of values – whilst it may be feasible to identify a common set of motivators in the workplace, we would argue that it is more difficult to pin down a common set of motivators in the technology sphere, particularly when considering different publics – each with their own set of needs. But it is important to at least outline the forms of social or consumer value that might help or hinder the uptake of future identity technologies. Our participants sometimes expressed these benefits in social terms [e.g. crime reduction or an improvement to health services] although we should note that these social benefits might be set against a perceived potential loss of privacy, social capital or civil liberties. However in personal terms, we were able to identify three themes where participants became more excited about the possible uptake of new identity technologies. These three 'motivators' were: convenience, personalization and aesthetics.

5.2.1 Convenience

The tension between privacy, security and convenience is well established, with recommended identity management processes often being subverted because they simply are not convenient [Tam et al. 2010], so we know that simple usability or convenience factors can be very important to users. In the identity space, we find that quite extreme or invasive identity management techniques are made acceptable to some communities, simply because they would appear to make life easier. Thus we find that the most common response to body-based authentication was the convenience it could offer by removing the carrying of tokens:

"Well you often go to the bank and you haven't got the right things, you've got to go home and get them. If they said to me it would save all that..." [older adult, male, biometrics].

"Personally for me I thought if you have stuff in your finger it is much easier, it simplifies absolutely everything in life, it cuts everything down, if you are at the doctors, like 'beep' and I'm in, there is my medical history coming up on the screen" [teenager, male, microchip (personal access)].

"It is easy, you know, than carrying a bank card, passport and stuff like that. Just having a tattoo is easy. You have not got anything to carry around" [refugee, female, smart tattoo].

"It's easy, no need for card, no need for PIN number sort of thing" [refugee, female, microchip (personal access)].

We should bear in mind, however, that convenience is itself culturally constructed. We found that it was common in some communities to share identity tokens and PIN numbers between partners or family members. For these users, new identity technologies posed a threat to this valued 'sharing' and became anything but a convenient solution:

"For the card thing if I want my husband to do some shopping while I am at work he won't be able to do it. I have to go there and use my card then it is not convenient for me after eight o'clock I have made the food, having dinner, wash the dishes and then go if I am tired, I don't need to, I don't want to go but I have to" [BME woman, biometrics].

5.2.2 Personalization

We know that there is value in asking consumers to get personally involved in the design of a product. For example, Kamali and Loker [2006] found that those consumers who were involved in the design of an item of clothing not only valued the item more, but became more involved with the overall online shopping process. In a study exploring end-user needs around federated identity management, people expressed a similar desire to participate in the process of creating and modifying their digital identities - choosing appropriate forms that resonated with their 'real' selves [Satchell et al. 2006]. We find this same desire in our current study, where the ability to adapt or customize technology to suit the individual was sometimes seen as an important potential motivator for future acceptance:

"I like the idea of having something to personalize; like James could choose a ring or I could choose to have it in a bracelet or something. So something that is personal to you, so it's not generic, not everybody has got it and can't look for his chip and steal it off him" [NEET, female, smart wearables].

"I would like it. It might be nice, like 'Hi Amy. How are you today?' while you are scanning your items…" [NEET, female, biometrics (face recognition)].

The need to disguise identity jewelry was also raised here – with participants stressing that identity technology should take different forms so that it wouldn't be easily recognized as such:

> "It would have to be better looking than that [RFID ring]. Also, looking like a ring, so that a thief wouldn't say "oh, that's one of those rings, I'll have that". So yes, it would have to look like a nice ring" [older adult, female, smart wearables].

We also noted different responses to the sense of permanent or temporary body art or wearables – influenced in part by an individuals' appetite for change, but also heavily modulated by culturally constructed beliefs about the integrity of the body:

> "I don't wear my ring you know… I will choose next week something else I am going to wear. And this is like it is quite ugly as well even if it is free, unless there are some diamonds in there! But you know, we don't use it, after one month we would want to change it for something different" [BME woman, smart wearables].

> "Some women they are religious, they cover their self and they don't want to show their hand or body to anyone else to scan it so that would be a problem" [BME woman, smart tattoo].

5.2.3 Aesthetics

A significant literature recognizes that strong individual and cultural differences can underpin consumer taste and that this in turn can play a major role in the hedonic response to different products [e.g. Hoyer and Stokburger-Sauer 2012]. The differentiation between functional and hedonic products is an important consideration for our research. Utilitarian or functional products are seen as a means to an end, whereas hedonic products are said to provide a more experiential and emotional value. This difference was active in the discussion around jewelry where the motivations around both beauty and emotional attachment were discussed:

> "Could it be put into anything or does it have to be plastic?" [older adult, male, smart wearables].

> "I mean you could have a ring that was your mother's or something that you always wear and it could go into something like that" [older adult, female, smart wearables].

We observed a tension between a traditional vs. modern aesthetic that played out differently across communities [particularly older vs. younger adults] and across contexts. Whilst the definition of 'aesthetic' varies in consumer literature, we consider it 'something positive, somehow related to beauty, with an inherent positive valence' [p.168, Hoyer and Stokburger-Sauer 2012]. Taste and aesthetics are often used interchangeably [Sibley 1959]. The greatest consensus was found following some very active discussions around the aesthetics of digital legacy or memorial technologies, where the appeal to tradition dominated. Specifically, digitally enhanced gravestones that could communicate identity information about the deceased were generally held to be 'creepy' and were seen as a step too far in terms of good taste:

"That's quite a traditional really kind of intrinsic part of British/Western culture of burying somebody. And I think to then slap a modern – ah it's just too much of a clash of old and new" [NEET, female, QR gravestone].

"I think have the QR reader in your home because then it'll fit in with your modern technology, but don't put it on graves or an urn" [NEET, female, QR gravestone].

6. GENERAL DISCUSSION

We have covered a lot of ground in this paper and we will use this general discussion to pull together a number of themes. We have described in detail a rigorous scenario sourcing exercise, which led to a framework of scenarios and artefacts that captured innovation in the identity space. We used these as probes and provocations in an inclusive design process with six marginalized community groups. In this discussion, we will firstly return to the issue of inclusive design and VSD to explore the extent to which such approaches add to our work, giving due consideration to Le Dantec's [2012] notion of publics in community engagement. Secondly, we will reflect on the utility of Herzberg's two-factor theory as a framework in which to represent citizen values in the identity space, linking to other recent work which might give additional insight to the utility of Herzberg's distinction. We will then consider the design and policy implications of the work we present here, using illustrative examples from the biometrics industry, before presenting final thoughts on the limitations and future directions for this work.

We have argued that our approach embraces both inclusive and value sensitive design philosophies. It is inclusive in the sense that we are trying to capture a set of design recommendations [below] that can address the needs of the many by having given full consideration to the needs of the few – seeking a 'plurality of voices, opinions and positions' [Le Dantec & DiSalvo 2013] from those publics facing citizenship challenges of various forms. It is value sensitive in the sense that we are addressing the impacts of identity technologies in the longer-term, recognizing a wide range of stakeholders and adopting a methodology that encourages an explicit expression of values. Our work also reflects some of the approaches employed by VSD practitioners. For example VSD practice may elicit 'dams' [design elements that are widely disliked] and 'flows' [design elements that are widely liked] and use these to shape a design process [e.g. Denning et al. 2010]. We have encouraged our participants to be clear about their likes and dislikes in the identity space, but have also encouraged a more explicit focus upon the *elements* of a particular design that might cause delight or concern. In another technique, VSD may seek to elicit 'value tensions' where the values of the individual may conflict with the group, or where there are inequalities among those who contribute to or benefit from the system [e.g. Miller et al. 2007] – recognizing that such tensions must be addressed in system design before it is likely to be accepted. We have certainly seen these value tensions played out in the identity space where the implementation of an identity system can lead to loss of autonomy and isolation, a loss of trust or public rejection [Whitley et al. 2014]. In adopting Herzberg's two factor framework we recognize that value tensions can exist in the hygiene space, but these are more likely to reflect the tension between what citizens may find acceptable and 'legitimate' and what is effective or efficient for government or business. In the 'motivation' space, the tensions between individuals or communities are likely to be more palpable and we

would anticipate some disagreement as to what might constitute an engaging, attractive or convenient identity technology [with 'smart' tattoos providing a pertinent example].

We argue, then, that there exist a set of values that are universal in the sense that they would underpin any effective and acceptable identity system. We have used 'hygiene factors' after Herzberg [1966] to describe the set of values that seems to underpin the most basic levels of acceptability of an identity management system. While Herzberg's two factor theory has been subject to critique [Bockman 1971] it has become more popular in recent years where it has become a valuable construct in positive psychology [whose proponents recognize that unhappiness is not simply the absence of happiness – see Sachau 2007], in marketing [adding to our understanding of customer loyalty] and in HCI [in elucidating design values]. Thus, for example, the marketing literature has identified customer satisfaction as a hygiene factor in the development of loyal customer relationships [Agustin and Singh 2005], while, within the HCI community, Sewchurran and Brown [2011] have identified a number of hygiene factors in service design and delivery which include the existence of a good governance framework underpinning the service, good alignment with the needs of the user, the users' perceptions of the competence of management to deliver the service and good cohesion in technical team support. Added to this, Zhang and von Dran's [2000] study has shown the importance of hygiene factors such as security, privacy, technical competence, impartiality and credibility for web design - rather similar to the constructs of legitimacy and competence we see here.

Hygiene factors alone are unlikely to motivate users to adopt new identity systems as they come online. Indeed, they are more likely to be associated with an absence of 'red flags' that would trigger citizen concerns. If we look back on our observations in this study, we can see these concerns expressed in the language of worry: 'how much will it cost?'; 'will it work?'; 'what if it goes wrong?'; 'will I be able to use it?'; 'what if I lose it'; 'what if someone steals it'; 'will it cause harm?'. In marked contrast, we have also identified a set of motivating factors, addressing issues of convenience, personalization and taste - where we see a rather different tone of evaluative expression: 'it looks nice'; 'it's too ugly'; 'I'd like it'; 'it would be easy'; 'it's not convenient'; 'I could personalize it' that shows users engaged in the language of choice. Here too we can recognize the lack of community consensus – the act of choice can reflect the values of the community as well as the individual. An implant may seem a convenient means of paying for drinks in a bar to a young adult [Michael & Michael 2010] and may even be considered acceptable as a means of tracking the whereabouts of vulnerable older adults, but it would also negate certain forms of token sharing that are considered essential in extended families. Similarly, a smart tattoo may seem both convenient and 'cool' to a fashion-conscious individual who follows innovative trends, but would be abhorrent to anyone with a religious prohibition on different forms of bodily mutilation.

Of course it is in just this type of audience segmentation that the commercial success of future identity technologies may depend. In this, our study reflects other work in HCI where Herzberg's model has been applied to mobile phone usage, to help differentiate between a number of 'core' [hygiene] attributes of mobile phones [safety and security, good organization] and a set of 'additional' motivators that influence purchase and use behavior [van Biljon et al. 2008] – the latter including aesthetics [ring tone, appearance], convenience [m-commerce] and personalization [the ability to create and maintain a personal history]. Or to the 'motivators' in web design, which

include fun, enjoyment user empowerment and a strong sense of reward [Zhang and von Dran 2000].

6.1 Design and Policy Implications

This brings us to a discussion of the design and policy implications of the work we have presented here. While it would be difficult to articulate a consistent message around our differentially valued 'motivators' it is worth pulling together some recommendations around the various hygiene factors identified here. We arrived at these recommendations by closely following our data, considering the issues arising from our workshops, and translating these into realistic targets for consideration within identity management technology design. In VSD terms, we have identified the following design 'flows' that would promote system acceptance.

- **Data segregation**: Adopt a principle of proportionality and only store data that is essential for the service or organization. Establish clear lines of accountability for data use.

- **Data Integrity**: Implement good data checking procedures. Where viable, provide a mechanism for people to update their personal data.

- **Data Access**: Ensure a clear data access policy and procedure. Provide information about who has access to personal information, and about why, when and how the data will be used.

- **Trust**: Consider trust in both the technologies and the people involved in designing and modifying the service. Establish an audit procedure to minimize potential for data loss.

- **Reliability**: Consider post-implementation issues around everyday use and issues of scale. Who takes responsibility for effective service delivery? Who is accountable for failure?

- **Security**: Provide transparency about system vulnerabilities- make people aware of risks and what could happen in the event of an online attack.

- **Safety**: Consider human vulnerabilities and physical hazards - make any health risks transparent.

- **Opt in**: Consider legal and governance frameworks to protect individuals- offer alternative solutions and informed consent. Have awareness of new social norms and recognize actual rather than idealized use of systems in the real world.

- **Diversity & Exclusion**: There may be a range of barriers to technology use- physical, financial, psychological- design to maximize accessibility for all. The provision of alternatives will encourage more widespread adoption.

We might assume that government and industry policy documents would show some sensitivity to the hygiene factors we have captured here – and indeed, across a range of international policy documents we can see that issues such as data segregation are

well-rehearsed. If we take an example from the biometrics industry, which is generally considered to be well-regulated, having articulated a number of important policy initiatives that drive design and implementation, then we can see a good alignment with some of the key issues we have raised here. In particular, our hygiene factors reflect three key principles captured in the Biometrics Institute's Privacy Guidelines [Biometrics Institute 2013]. First is the principle of proportionality – we have noted that an identity system will only have legitimacy if there is balance between the benefits associated with that system and the technological power brought to bear in designing and implementing the system – in other words, identity solutions should not be over-engineered and the data collected should be contextually appropriate. Second is the principle of informed consent – resonating with our claims around the importance of knowing who has access to our identity data and the need for choice in opting in or out of systems, and finally the principle of truth and accuracy in business operations which reflects our discussion of the importance of competence in the effective roll out of any identity management system. Again, in the biometrics world we have seen that the perceived trust and robustness of biometrics against privacy attacks is an important factor for acceptance [El-Abed et al. 2012].

6.2 Limitations and future work

In terms of limitations of this work, we recognize that six minority groups is by no means comprehensive and a self-selecting bias may mean that, even within these six communities, we may not have fully captured the relevant attitudes and concerns. Nevertheless, by considering the needs of a very diverse few, we believe we have drawn out a number of novel themes and have set them against a backdrop of an appropriate theoretical framework. As we have argued throughout this paper, recognizing the concerns of diverse segments of society is a recognized principle in inclusive design, allowing for the exploration of extremes that can hopefully benefit wider society.

When working in the IM technology space, developments are rapid. This work was conducted over a two-year period, and therefore our scenario sourcing exercise provided examples for our workshops most suitable *at that time*. The duration of the project meant that new technologies appeared whilst data collection was ongoing. That said, we did observe saturation in our data analysis – i.e. we saw the same themes emerging across quite diverse technologies and would not anticipate much benefit from the addition of further scenarios.

Thinking about future work, we have underlined the importance of legitimate, reliable systems that facilitate citizen choice but have given a more complex message regarding those motivators likely to encourage engagement with new identity technologies. Those involved in the development of identity technologies should ensure they get the basics of governance absolutely right before a more nuanced consideration of the way that different communities or different 'market segments' may be motivated to adopt new systems. We believe that the practice of eliciting design values from our more marginalized communities – designing from the outside-in as it were – has proved useful in offering important insights that align well with both industry and community needs. This is important when we remember that identity technologies are becoming ubiquitous, but when taken in the round, have had a very mixed public response. There is nothing surprising here - the rollout of new identity bureaucracies has always been politically fraught [e.g. Caplan and Torpey 2001] but there is a paradox that lies at the heart of identity management

that embraces both the public rejection of government-led systems such as identity cards [in the UK at least] and the widespread adoption of business-led systems such as loyalty cards and social media platforms for the expression of self. Understanding more about both the universal and the diverse values that underpin this paradox will take us one step closer to acceptable and even enjoyable identity design.

REFERENCES

Clara Agustin and Jagdip Singh. 2005. Curvilinear effects of consumer loyalty determinants in relational exchanges. *J. Marketing Res.*, 42, 1, 96-108. DOI: http://dx.doi.org/10.1509/jmkr.42.1.96.56961

Tamara Alsheikh, Jennifer Rode and Siân Lindley. 2011. [Whose] Value-Sensitive Design: A Study of Long-Distance Relationships in an Arabic Cultural Context. In *Proceedings of the 2011 ACM conference on Computer Supported Cooperative* Work [CSCW '11], ACM Press, 75-84.

Biometrics Institute Privacy Guidelines. 2013. Retrieved June 16, 2014 from http://www.biometricsinstitute.org/pages/privacy-charter.html

David G. W. Birch. 2009. Psychic ID: A blueprint for a modern national identity scheme. *Identity in the Information Society*, 1, 1, 189–201.

Valerie M. Bockman. 1971. The Herzberg Controversy. *Pers. Psychol.*, 24, 2, 155-189.

Alan Borning and Michael Muller. 2012. Next steps for value sensitive design. In *Proceedings of the ACM Conference on Human Factors in Computing Systems [CHI '12],* ACM Press, 1125-1134.

danah boyd and Alice Marwick. 2011. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, September 22, 2011, Oxford Internet Institute, UK.

Virginia Braun & Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3, 2, 77–101. DOI: 10.1191/1478088706qp063oa

Pam Briggs. 2013. Future Identities: Changing identities in the UK– the next 10 years. DR 4: Will an increasing element of our identity be 'devolved' to machines? *Government Office for Science: Foresight Report,* January 2013.

Pam Briggs, Mark Blythe, John Vines, Stephen Lindsay, Paul Dunphy, James Nicholson, David Green, Jim Kitson, Andrew Monk and Patrick Olivier. 2012. Invisible design: Exploring Insights and Ideas through Ambiguous Film Scenarios. In *Proceedings of conference on Designing Interactive Systems [DIS '12]*, ACM Press, 534-543.

Pam Briggs and Patrick Olivier. 2008. Biometric daemons: authentication via electronic pets. *In Proceedings of conference on Human Factors in Computing Systems [CHI EA 2008],* ACM Press, 2423–2432. DOI: 10.1145/1358628.1358699

Jan Camenisch, Simone Fischer-Hübner, & Kai Rannenberg. 2011. [Eds.]. *Privacy and Identity Management for Life*. New York/Heidelberg: Springer Press.

Jane Caplan and John C. Torpey [Eds.]. 2001. Documenting individual identity: The development of state practices in the modern world. Princeton: Princeton University Press.

Gilbert Cockton. 2006. Designing Worth is Worth Designing. In *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles [NordiCHI '06].* ACM Press, New York, NY, 165-174. DOI: 10.1145/1182475.1182493

Christopher A. Le Dantec. 2012. Participation and publics: supporting community engagement. *In Proceedings of the ACM Conference on Human Factors in Computing Systems [CHI '12],* ACM Press, 1351–1360. DOI: 10.1145/2207676.2208593

Christopher A. Le Dantec and Carl DiSalvo. 2013. Infrastructuring and the formation of publics in participatory design. *Soc. Stud. Sci.*, 43, 2, 241–264. DOI: 10.1177/0306312712471581

Christopher A. Le Dantec, Erika Shehan Poole and Susan P. Wyche. 2009. Values as lived experience: evolving value sensitive design in support of value discovery. In *Proceedings of the ACM Conference on Human Factors in Computing Systems [CHI '09],* ACM Press, 1141–1150. DOI: 10.1145/1518701.1518875

Tamara Denning, Alan Borning, Batya Friedman, Brian T. Gill, Tadayoshi Kohno and William H. Maisel. 2010. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the ACM Conference on Human Factors in Computing Systems [CHI '10],* ACM Press, 917-926. DOI: 10.1145/1753326.1753462

Bruce Eckfeldt. 2005. What does RFID do for the consumer? *Comm. ACM*, 48, 9, 77–79.

Mohamad El–Abed, Romain Giot, Baptiste Hemery and Christophe Rosenberger. 2012. Evaluation of biometric systems: a study of users' acceptance and satisfaction. *International Journal of Biometrics*, 4, 3, 265-290. DOI: 10.1504/IJBM.2012.047644

Carlos Flavián and Miguel Guinalíu. 2006. Consumer trust, perceived security and privacy policy. *Ind.*

Manage. Data Syst. 106, 5. 601-620.
Foresight Future Identities 2013. *Future Identities: Changing identities in the UK– the next 10 years*. Final Project Report. The Government Office for Science, London.
Batya Friedman. 1996. Value-sensitive design. *interactions*, *3*, 6, 16-23. DOI: 10.1145/242485.242493
Batya Friedman and Peter H. Kahn Jr. 1992. Human agency and responsible computing: Implications for computer system design. *J. Syst. Software*. 17, 7–14. DOI: 10.1016/0164-1212(92)90075-U
Batya Friedman, Peter H. Kahn Jr. and Alan Borning. 2006. Value Sensitive Design and Information Systems. In P. Zhang and D. Galletta [Eds.], *Human-Computer Interaction in Management Information Systems: Foundations,* 348-372. Armonk, New York.
Gartner. 2012. Gartner Identifies Six Trends That Will Drive the Evolution of Identity and Access Management and Privacy Management in 2012. Retrieved December 12, 2012 from http://www.gartner.com/it/page.jsp?id=1909714
Anthony Giddens. 1991. Modernity and Self-Identity: Self and Society in the Late Modern Age, Stanford, CA: Stanford University Press.
Erving Goffman. 1959. *The Presentation of Self in Everyday Life* [4th ed.]. Penguin.
Joy Goodman, Hua Dong, Peter Langdon and John P. Clarkson. 2006. *Factors involved in industry's response to inclusive design*. In John Clarkson, Patrick Langdon and Peter Robinson [Eds.], Designing accessible technology. London: Springer-Verlag. DOI: 10.1007/1-84628-365-5_4
GOV.UK. 2014. Identity assurance: delivering trusted transactions. Retrieved December 11, 2014 from https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions
Frederick Herzberg. 1966. *Work and the Nature of Man*. Cleveland, OH: World.
Frederick Herzberg. 1987. One more time: How do you motivate employees? *Boston: Harvard Business Review*. 46-57.
House of Commons Science and Technology Committee, Responsible Use of Data. Retrieved November 19, 2014 from http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf
House of Lords report. 2014. EU Data Protection law: a "right to be forgotten"? European Union Committee. Retrieved November 19, 2014 from www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf
Wayne D. Hoyer and Nicola E. Stokburger-Sauer. 2012. The role of aesthetic taste in consumer behavior. *J. Acad. Market. Sci*., 40, 1, 167-180.
Narges Kamali and Suzanne Loker. 2006. Mass Customization: On-line Consumer Involvement in Product Design. *J. Comput-Mediat. Comm*. 7, 4. DOI: 10.1111/j.1083-6101.2002.tb00155.x
Noriaki Kano, Nobuhiku Seraku, Fumio Takahashi and Shinichi Tsuji. 1996. *Attractive quality and must-be quality*. In John D. Hromi, [ed.]: The Best on Quality. Vol. 7. ASQC Quality Press, Milwaukee.
Marija Krlic. 2014. Social costs of surveillance and the case of biometrics. In Proceedings of 37th International Convention on Information and Communication Technology, Electronics and Microelectronics [MIPRO '14], 1278-1282. IEEE. DOI: 10.1109/MIPRO.2014.6859764
Jonathan Lazar [Ed.]. 2007. Universal usability. Designing Computer Interfaces for Diverse User Populations. Wiley.
Siân Lindley, Catherine C. Marshall, Richard Banks, Abigail Sellen and Tim Regan. 2013. Rethinking the Web as a Personal Archive. *International World Wide Web Conference, [WWW '13].* 749-759. DOI: 978-1-4503-2035-1 /13/05
Silvia Lindtner, Judy Chen, Gillian R. Hayes and Paul Dourish. 2011. Towards a framework of publics: Re-encountering media sharing and its user. *ACM Trans. Comput.-Hum. Interact*. 18, 2, 5. DOI: 10.1145/1970378.1970379
Linda Little, Elizabeth Sillence and Pam Briggs. [2009]. Ubiquitous Systems and the Family: Thoughts about the Networked Home. In *Proceedings of the 5th Symposium on Usable Privacy and Security [SOUPS 2009*], 6. DOI: 10.1145/1572532.1572540
Kai-Uwe Loser and Martin Degeling. 2014. *Security and Privacy as Hygiene Factors of Developer Behavior in Small and Agile Teams*. In Kimppa, K., Whitehouse, D., Kuusela, T., Phahlamohlaka, J. [eds.] ICT and Society. 431, 255-265. Springer Berlin Heidelberg.
Mary Madden. 2014. *Public Perceptions of Privacy and Security in the Post-Snowdon Era*. Pew Research Center Report. Retrieved May 19, 2015 from http://pewrsr.ch/1EtEBRh
Clara Mancini, Yvonne Rogers, Arosha K. Bandara, Tony Coe, Lukasz Jedrzejczyk, Adam N. Joinson, Blaine A. Price, Keerthi Thomas and Bashar Nuseibeh. 2010. Contravision: exploring users' reactions to futuristic technology. In *Proceedings of the ACM Conference on Human Factors in Computing Systems [CHI '10],* ACM Press, 153-162. DOI: 10.1145/1753326.1753350
Daniel A. McAdams and Vincent Kostovich. 2011. A framework and representation for universal product design. *Int. J. Des*, 5, 1, 29-42.
D. Harrison McKnight, Vivek Choudhury and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. Inform. Syst. Res., 13, 3, 334-359. DOI: 10.1287/isre.13.3.334.81
Katina Michael and MG. Michael. 2010. The Diffusion of RFID Implants for Access Control and

ePayments : A Case Study on Baja Beach Club in Barcelona. *IEEE Symposium on Technology and Society*, 242–252. Singapore: IEEE.

Katina Michael and MG. Michael. [Eds.]. 2014. *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies*. IGI Global- Advances in Human and Social Aspects of Technology (AHSAT).

Jessica K. Miller, Batya Friedman, Gavin Jancke and Brian Gill. 2007. Value tensions in design: the value sensitive design, development, and appropriation of a corporation's groupware system. In *Proceedings of the 2007 international ACM conference on Supporting group work [GROUP '07],* 281-290. ACM Press. DOI: 10.1145/1316624.1316668

Lisa P. Nathan, Batya Friedman, Predrag Klasnja, Shaun K. Kane and Jessica K. Miller. 2008. Envisioning Systemic Effects on Persons and Society throughout Interactive System Design. In *Proceedings of conference on Designing Interactive Systems [DIS '08],* ACM Press, 1-10. DOI: 10.1145/1394445.1394446

Alan F. Newell. 1995. *Extra-ordinary Human Computer Interaction*, in Edwards, A. D. N. [Ed.], Extra-ordinary Human-Computer Interaction. Cambridge University Press.

Alan F. Newell and Peter Gregor. 1997. *Human computer interfaces for people with disabilities* in Helander, M., Landauer, T.K. and Prabhu, P. (eds), Handbook of Human-Computer Interaction. Elsevier Science. 813-824.

Alan F. Newell and Peter Gregor. 2000. User Sensitive Inclusive Design – in search of a new paradigm. In *Proceedings on the 2000 conference on Universal Usability [CUU '00],* ACM Press, 39-44. DOI: 10.1145/355460.355470

Alan F. Newell, Margaret E. Morgan, Peter Gregor and Alex Charmichael. 2006. Theatre as an intermediary between users and CHI designers. In *Proceedings of conference on Human Factors in Computing Systems [CHI EA '06*], ACM Press, 111-116. DOI: 10.1145/1125451.1125479

Helen Nissenbaum. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books.

Bas Raijmakers, William W. Gaver and John Bishay. 2005. Design documentaries: inspiring design research through documentary film. In *Proceedings of conference on Designing Interactive Systems [DIS 2005*], ACM Press, 229-238. DOI: 10.1145/1142405.1142441

Christine Satchell, Graeme Shanks, Steve Howard and John Murphy. 2006. Beyond security: implications for the future of federated digital identity management systems. In *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments [OZCHI '06],* ACM Press, 313-316.

Theresa Satterfield. 2001. In Search of Value Literacy: Suggestions for the Elicitation of Environmental Values. *Environ. Value*. 10, 3, 331-359.

Daniel A. Sachau. 2007. Resurrecting the motivation-hygiene theory: Herzberg and the positive psychology movement. *Human Resource Development Review*, 6, 4, 377-393. DOI: 10.1177/1534484307307546

Eureka Sewchurran and Irwin Brown. 2011. Successful ICT service delivery: enablers, inhibitors and hygiene factors: a service provider perspective. In *Proceedings of the South African Institute of Computer Scientists and Information Technologists Conference on Knowledge, Innovation and Leadership in a Diverse, Multidisciplinary Environment [SAICSIT '11].* ACM Press, 195-204. DOI: 10.1145/2072221.2072244

Ben Shneiderman, B. 2000. Universal usability. *Commun. ACM*, 43, 5, 84-91. DOI: 10.1145/332833.332843

Frank Sibley. [1959]. Aesthetic concepts. *Philos. Rev*., 68, 421– 450.

Yogendra Narain Singh. 2011. Challenges of Unique ID Environment. In *Proceedings of National Conference UID*. Impact of Aadhaar in Governance, Computer Society of India Lucknow.

Take This Lollipop. Retrieved June 19, 2014 from www.takethislollipop.com.

Leona Tam, Myron Glassman and Mark Vandenwauver. 2010. The psychology of password management: a trade-off between security and convenience. *Behaviour & Information Technology*, 29, 3, 233-244. DOI: 10.1080/01449290903121386

Sherry Turkle. 2012. Alone together: Why we expect more from technology and less from each other. Basic books, New York.

Judy van Biljon, Paula Kotzé and Karen Renaud. 2008. Mobile phone usage of young adults: the impact of motivational factors. In *Proceedings of the 20th Australasian Conference on Computer-Human Interaction: Designing for Habitus and Habitat [OZCHI '08]*. ACM Press, 57-64.

Gregg Vanderheiden. 2000. Fundamental principles and priority setting for universal usability. In *Proceedings on the 2000 conference on Universal Usability [CUU '00],* 32-37. ACM Press. DOI: 10.1145/355460.355469

Liesbet VanZoonen, Pam Briggs, Aletta Norval, Sandra Wilson, Lilia Gomes-Flores, Jasmine Harvey, Dougie Kinnear, Elpida Prasopoulous, Lisa Thomas, Georgina Turner and Sharon Walker. 2013. *Scenarios of identity management of the future*. Retrieved June 18, 2014 from http://www.imprintsfutures.org/brochures/

Lynne M. Vieraitis, Heith Copes, Zachary A. Powell and Ashley Pike. 2014. A Little Information Goes a

Long Way: Expertise and Identity Theft. *Aggress. Violent Beh.* 20, 10-18. DOI: 10.1016/j.avb.2014.12.008

John Vines, Mark Blythe, Stephen Lindsay, Paul Dunphy, Andrew Monk and Patrick Olivier. 2012. Questionable Concepts: Critique as a Resource for Designing with Eighty Somethings. In *Proceedings of the ACM Conference on Human Factors in Computing Systems [CHI '12]*, ACM Press, 1169–1178. DOI: 10.1145/2207676.2208567

Edgar A. Whitley, Uri Gal and Annemette Kjaergaard. 2014. Who do you think you are? A review of the complex interplay between information systems, identification and identity. *Eur. J. Inform. Syst.*, 23, 1, 17-35.

Ping Zhang and Gisela M. von Dran. 2000. Satisfiers and dissatisfiers: A two-factor model for website design and evaluation. *J. Am. Soc. Inform. Sci.*, 51, 14, 1253-1268. DOI: 10.1002/1097-4571(2000)9999:9999<::AID-ASI1039>3.0.CO;2-O

V. Zorkadis and P. Donos. 2004. On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security*, 12, 1, 125–137.