Poster: Identity Management Futures: Assessing Privacy and Security Concerns of the Young and Old

Lisa Thomas & Pam Briggs
PaCT Lab, Psychology Department
Northumbria University
lisa.thomas@northumbria.ac.uk

1. INTRODUCTION

'IMPRINTS' is a three-year research project which aims to understand public expectations about identity management (IdM) technologies in the future. This paper will describe how the project is exploring desires and taboos for the public regarding their IdM in the future.

Identity management is thought of as the ways in which we authenticate ourselves, or simply how we can prove we are who we say we are. This kind of IdM is often carried out in order to reduce cost or minimize repetition. For example, people currently have usernames and passwords to access online services. In the future, we might envisage some kind of alternative biometric process to reduce this effort. The technologies that are linked with IdM practices may also take the form of 'smart' tokens like ID or customer cards, jewellery, garments, or enhanced smart phones.

To date, there has been no comprehensive body of research that offers an understanding of public responses to various forms of near-future identity management scenarios. Nevertheless, the idea of future gazing, or 'futurology' has been recognized as a valuable way to think about how things might change [3].

In order to consider IdM practices of the future, issues of privacy and security are key- for example, if we are required to use biometrics to authenticate ourselves at the airport, who will be able to see that information? How can we be sure that any database of our fingerprints will be kept securely? Will the public accept the use of their private online information for public services? In order to understand some of these issues, focus groups with young and old residents in Newcastle upon Tyne.

2. RESEARCH BACKGROUND

IdM technologies are developing and changing rapidly, yet our understanding of public attitudes towards these changes is minimal. Whilst the academic literature surrounding new IdM technologies may be lacking, there is a plethora of blogs, articles and news reports describing a multitude of technologies for the future, and their potential security pitfalls. As an example, in 2013 reviews of Google Glass have permeated the news, and assessments of the technology have been made well before its actual release date [2].

However, much of the writing about new and developing technologies is based on presumption. Our research aims to find out how these hypothesized futures might be received by the public, with our research question being:

'How might people engage/disengage with identity management practices, services and technologies of the future?'

2.1 Research Framework

This first phase of the research project was to understand the kinds of IDM scenarios present in psychology, media, design and political arenas. The project team developed a research framework which would enable the IdM technologies encountered in the literature to be classified (see Figure 1).

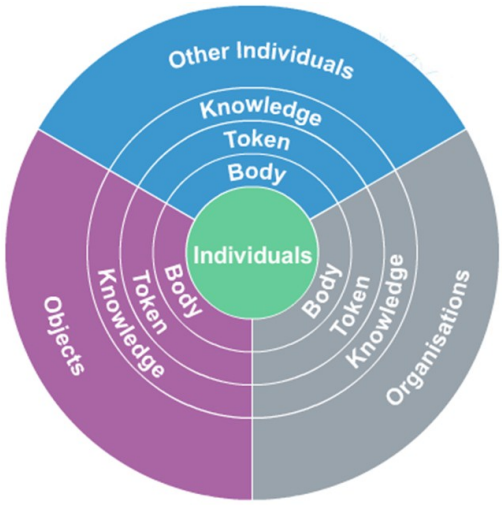

Figure 1. The IMPRINTS scenario framework

The grid portrays two aspects of IdM:

1. **Who might we interact with?** This can either be an interaction with static objects, other individuals, or organisations.

2. **What form does that interaction take?** We may use tokens such as a passport to prove our identity; we may use our body e.g. facial recognition, to identify ourselves; or we may use our knowledge of information such as passwords and PINs to validate who we are.

These combinations of 'who' and 'what' led to the development of a core set of 12 scenarios (see [4] for more detail).

3. METHODS

3.1 Stimuli

Using the research framework as a guide, the team searched for technologies that were being presented as a possible solution or enhancement for IdM in the future. Some of these technologies were then chosen for inclusion in focus groups. A number of methods were used to engage participants, including film clips,

artifacts and paper exercises. Fig. 2 and 3. show examples of the kind of stimuli used: a 'PsychicID card' [1] and QR code-enhanced gravestone. The PsychicID card is designed to reveal only the necessary information in a given situation, allowing a minimal amount of information to be disclosed. The card could be used to access to a nightclub, or to register at the doctors, for example. The QR code gravestone is a way to convey information about a deceased friend or relative to others in the form of a blog or Facebook page. The QR code is placed on a headstone to be scanned.

Figure 2. The PsychicID card

Figure 3. QR gravestone

3.2 Participants

Five focus groups were conducted, two with teenagers [n=10] and three with older adults [n=18] from the Newcastle area. Participants ranged from 16 to 85 years old.

4. RESULTS

The focus groups were recorded, transcribed, and analysed using NVivo software and a thematic approach. The data from transcripts were organized into factors and refined by two IMPRINTS researchers. Initially 28 factors have been identified. These factors have been organised into clusters based on their desirable or undesirable nature. Some examples include:

+	-
Elegance/cool design	Nanny state/public harm
Data responsibility	Exclusion from technology
Trusted people	Bad taste/creepy design
Public good	Cost of change/inertia

Whilst these factors are still being refined, it is worthwhile noting initial findings and the emerging privacy and security considerations of the participants. The notion of '*who sees?*' and '*in what context?*' was important for both age groups. Participants had a clear idea of who could be trusted with their identity data, and who would be given access (family, doctors), yet had a lack of trust in bigger organizations and the government, citing security breaches as a concern. The amount of control that would be exercised was a big consideration, and with the ability to personalize and manage their own information, participants reported feeling more comfortable with the technologies.

If participants felt that an IdM technology would provide them with a benefit, such as the medical microchipping of Alzheimer's patients, then an invasion of privacy could be tolerated. However, concepts such as Google Glass, where the usefulness of the technology was debated, any invasion of privacy was deemed unnecessary. Participants often reported that they lacked trust in the existing databases or government services, and cited security breaches as a reason for hesitation regarding large biometric-gathering technologies.

5. DISCUSSION

This research has allowed us to better understand the taboos and desires of the general public regarding IdM technologies of the future. Participants expressed a desire for some technologies, yet a distinct distaste for others. One criticism of the scenarios presented was the unknown privacy and security issues- people were not sure who would be seeing their personal data, or how it would be used. Addressing these queries is so important, before the implementation of such technologies. This research is now continuing with underrepresented populations, such as the homeless and refugees, with focus groups exploring the social and cultural implications of IdM technology of the future.

6. ACKNOWLEDGMENTS

We acknowledge the support of the RCUK Global Uncertainties Programme in funding the IMPRINTS project (EPSRC grant No. EP/J005037/1).

7. REFERENCES

[1] Birch, D. G. W. (2009). Psychic ID: A blueprint for a modern national identity scheme. Identity in the Information Society, 1(1), 189–201.

[2] Loveridge, S (2013). Google Glass privacy risks discovered by hackers. http://www.trustedreviews.com/news/google-glass-privacy-risks-discovered-by-hackers#AXGdm3P7Pdw6QHwk.99 Accessed 17th May 2013.

[3] Nicholas, L. (2013). Futurology: shining a bright, broad beam of light into the darkness. http://www.guardian.co.uk/science/political-science/2013/may/03/science-policy Accessed 17th May 2013.

[4] Van Zoonen, L. et al. (2012). Scenarios of identity management in the future. Accessed 17th December 2012 at http://www.imprintsfutures.org/senarios1/