Government Office for Science

Foresight

Future Identities: Changing identities in the UK – the next 10 years

DR 4: Will an increasing element of our identity be 'devolved' to machines?

Pam Briggs

Northumbria University

January 2013

This review has been commissioned as part of the UK Government's Foresight project, *Future Identities: Changing identities in the UK – the next 10 years.* The views expressed do not represent policy of any government or organisation.

Contents

1. Summary

The smartphone has emerged as one of the key machines of the 21st century. In this chapter, we explore they way in which it can facilitate four types of identity exchange: via the recording and transmission of personal histories, via the creation of personal profiles that reflect everyday behaviours, via membership of online social communities and via public rankings and reputation ratings. The resulting future vision is one in which identity is a distributed phenomenon, not easily controlled by a single individual.

2. Background

The first few years of the 21st Century saw the emergence of a series of futuristic scenarios, penned by researchers or designers working in industry, government and academia that attempted collectively to map out the promise of ubiquitous computing. This was the promise of a world in which computational intelligence moved away from artefacts that looked and behaved like computers to become embedded in everyday objects and environments. The scenarios predicted the rise of the smart home, in which temperature, lighting, entertainment and lifestyle functions were programmed to respond sensitively to the presence and behaviour of its various residents. The smart car, able to recognise who was at the wheel and capable of navigating seamlessly through diversions and heavy traffic and signalling car-sharing opportunities with like-minded others. The smart office, where full wall displays of the latest financial projections could be activated and casually manipulated with voice and gesture and the smart world of leisure, where taxis pre-programmed with a destination would whisk customers to pre-booked, preferred restaurants where the bill would be paid automatically (without recourse to money, credit card or cheque) upon exit.

These predictions form an interesting backdrop to current developments and one particular prediction can serve as an illustration of how well such scenarios have served as a roadmap to the present day. In 2006, in a report for FIDIS (the EU Funded Network of Excellence on the Future of Identity in the Information Society), Sabine Delaitre (2006) described the bar of the future. Specifically she asked *'What will it be like to walk into a bar in 2012?*' Her resulting scenario runs as follows: A customer enters the bar and declares his preferences using his 'personal digital assistant' or PDA which activates his availability to meet a friend and transmits data to the bartender: his favourite drink, his first language and any specifics such as prescribed medication and names of friends. The barman asks if he wants a cappuccino (the transmitted favourite drink), while the adaptive screen shows him the soft drinks option (it knows he cannot have alcohol because of his medication). He watches TV via the public screen whilst listening to a simultaneous translation in his native language. An alarm notifies him when any of his friends are in the vicinity. As he leaves, he can choose to pay with a fingerprint or Radio Frequency Identification (RFID) enabled card.

It is instructive to compare this scenario with the reality of 2012. Two things are particularly notable: firstly, the seamless transmission of user preferences to the barman (in the form of some kind of comprehensive identity profile, inclusive of medical data) doesn't ring true. Surprisingly, in an era where we are profligate with our personal data, it still seems far-fetched

to imagine that we would transmit medical data to a barman – and why wouldn't we simply *tell* the barman what drink we want, when we want it? Secondly, for 'PDA' we should read smartphone, as this has already become the device with the capacity to (i) authenticate the user via fingerprint or face recognition software; (ii) offer a simultaneous language translation; (iii) pay seamlessly for a drink or a meal without recourse to a credit card or cash (cf the pizza express app) and (iv) let friends know when the user is in a particular location and also alert the user if friends are near (via location-based technologies such as foursquare).

The smartphone is a particularly striking development when viewed through the lens of the recent past which foretold the rise of smart house, office or car, but stayed relatively silent on the evolution of the mobile phone. It has already become the major vehicle for identity management across social and organisational networks of various kinds. If we are to review the current state of the art in order to predict the kinds of identity work machines will deliver in the future, then we would do well to begin with an analysis of new kinds of functionality the smartphone or tablet offers when combined with cloud computing services.

3. Framework

A framework for understanding the different components of identity is shown in figure 1, below.

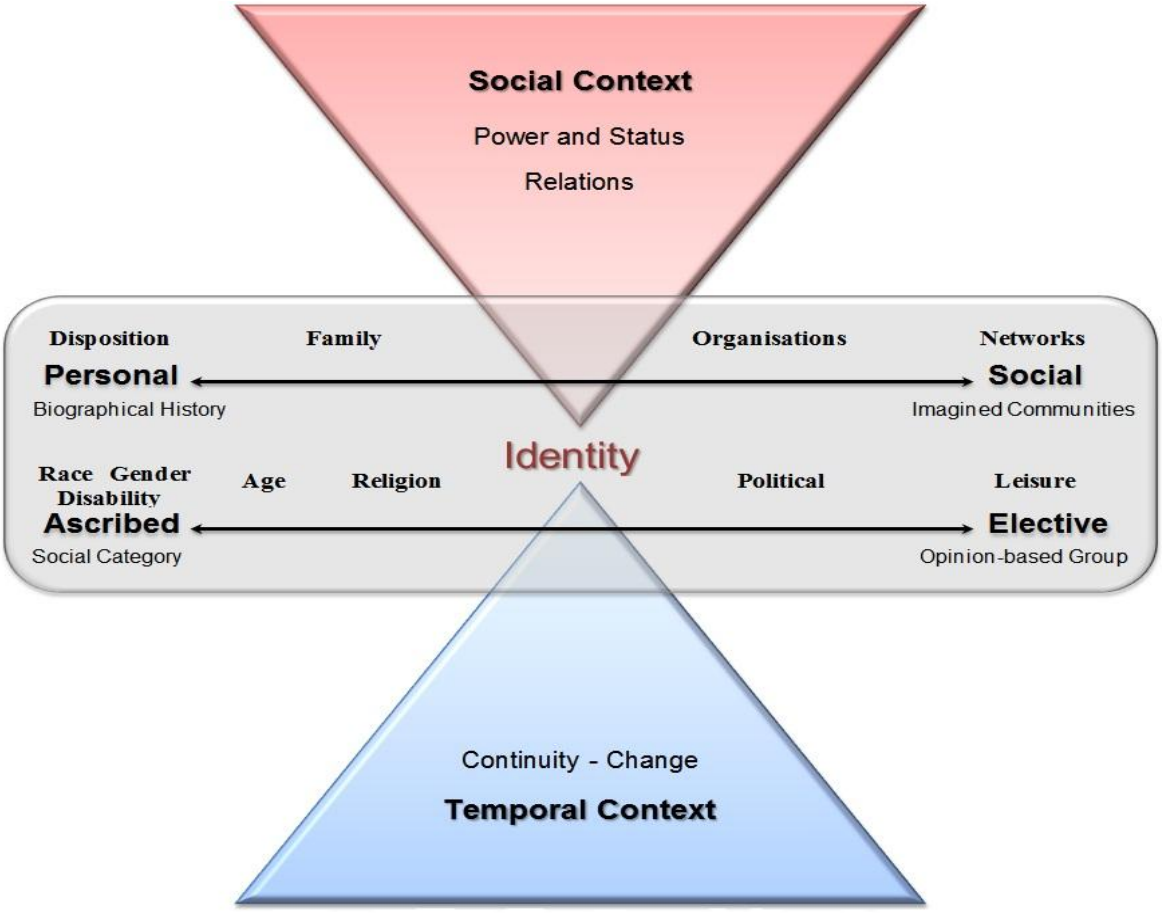

Figure 1: A working definition of identity

In the remainder of this paper, I will show how identity services can be mapped onto the framework's two identity dimensions (personal-social; ascribed-elective), so that it yields the four types of identity exchange that are likely to dominate our future: (i) curating and publishing personal histories and self-representations (Personal, Elective); (ii) profiling of personal and demographic data, online behaviours and interactions (Personal, Ascribed) (iii) affiliation to online social and information communities for the purposes of support, information and advice and the appropriation of personal experiences and opinions in decision-making via crowd-sourcing and sense-making processes (Social, Elective) and (iv) The use of reputation, rating and tagging systems as a means of public labelling (Social, Ascribed). Finally, I will consider the implications of managing such a complex identity information space and discuss the ways in which machines may come to support us in this process, by the use of personal agents offering privacy protection and identity management services.

3.1 Curating and publishing personal histories and self-representations (Personal, Elective)

We have recently seen the rise of 'life-logging' technologies and applications which offer individuals the opportunity to curate their own lives. Life logging is most frequently done through photographic and video collections which are publicly shared and tagged in such a way as to help others make sense of the recorded experience. Tagging is also the means by which an individual labels his or her life experiences in order to make sense of them at some future point. Clearly there are identity issues here, as individuals are using photos and tags not only as a means of defining and recording their identity, but also as a means of promoting a particular self-representation (e.g. Gulotta *et al*, 2012).

This curatorial work is gaining importance. YouTube and Facebook have developed new techniques for making private histories public, while Microsoft has a significant research agenda around life-logging and the personal or family curation of photographs and videos (e.g. Kirk and Sellen, 2010). Naturally there are concerns about privacy rights in this space and also issues about managing and censoring vast amounts of digital 'life'. Concerns about ownership have been also raised by Odom *et al*. (2012), who notes how impossible it is to really 'know where things live' in the cloud:

"two emergent themes run throughout: that posting something online, in today's world, can mean relinquishing control over the things that you care about, but also losing awareness of what exists, where it is, who has access to it, who is accountable for it, and what is being done with it."

The rules of digital possession are dramatically different to those of offline possession: once an image has been posted online it can't be completely retrieved – others can reproduce it and adapt or use it in ways which may be challenging to the original owner. The new 'Internet of things' contains many digital objects that have been placed in the hands of companies (facebook, flickr, dropbox) who could rescind the rights to them. There is evidence that such developments are challenging our notion of selfhood, but are also influencing our offline behaviour, such that our sense of what behaviours are appropriate in different situations is, in part, informed by the records that will be taken of such behaviour that may be subsequently used or appropriated by others (Joinson *et al*, 2011).

3.2 Profiling of personal and demographic data, online behaviours and interactions and social tagging of personal digital content (Personal, Ascribed)

Shared personal data can be used to generate a user profile that can arguably benefit both commerce and the consumer in terms of the provision of *personalised services*. An example of commercial benefit is Behavioural Advertising (BA) – a practice in which users are presented with ads based on information gleaned from past Internet browsing behaviours. Advertisers are able to use information about online behaviour to tailor ad content, subsequently influencing online purchasing behaviour. But one interesting aspect of this service is that the profiling process is largely hidden from the consumer - relatively few BA models being explicitly 'opt-in'. Here, then, we have identities being ascribed to a consumer without their knowledge or consent – a process which naturally triggers privacy concerns.

Many other services have an opt-in model, where consumers are openly invited to sign-up to personalised content. This can be successful in those domains where the user is flooded with choice, but where many of the available options are irrelevant. Broadcast television provides a good example: the number of television channels has multiplied and customers are also able to capture a great deal of content on video. Hence personalised services such as TiVo have been developed in order to help the viewer manage this complex space. TiVo can make recommendations by matching user likes and dislikes to a centralised database recording the preferences of like-minded others – a process known as 'collaborative filtering'. Such filtering processes can vary in their sophistication, but can only ever be as good as the profile data they can extract from their users. TiVo is rather crude in this respect and this led to a good deal of bad press when it was first launched, when a Wall St. Journal article offered readers advice on how to handle a TiVo that, on the basis of viewing preferences, erroneously "thinks you are gay" (Zaslow, 2002).

Contemporary profiles are typically more sophisticated and recent smartphone developments now offer organisations (and users) the potential to integrate online browsing histories with information about offline habits (work, shopping, leisure) via a process of location-tagging. Location services have been with us for a few years now. Early developments were aimed at vulnerable adults, lone-workers or children, but in the past year or two, location-services have found their way into everyday social networking applications, offering friends the opportunity to locate each other (foursquare) or, more menacingly, offering potential predators the opportunity to snoop on peoples' preferences and habits in some cases to identify potential sexual partners[1].

A recent industry report by Martin (2012) argued that a new location service called Placeme offers a serious glimpse into the future. Placeme can automatically publish daily timelines that describe where you are at different times of the day and stream this data to selected others. The developers assume that this information could be appropriated by consumer-focussed businesses, offering them the capability of locating a customer's current position in a particular store and offer competitive prices for products nearby. Developments of this type are interesting because they significantly enhance our ability to predict patterns of behaviour and personal preference in a way which is context sensitive (i.e. that reflect activities undertaken at a particular time and place). Systems such as placeme.com offer a seamless opportunity to make personal histories public, but such developments are best understood when we see how they sit within a larger trend (see above) in which people elect to publicise their private lives in the form of blogs (diaries), tweets, posted experiences, photos and videos and where these private histories can become public by a process of social appropriation. The power to combine such personal histories with rich contextual data suggests a future in which our daily habits and preferences can become highly accessible to others.

Consider: as more and more of our transactions are completed by mobile phone, then they become increasingly tied to a date and time stamp which can, in turn be supplemented by various other 'tags' that may represent who you were with or what you were doing (see Gasson *et al*, 2011). This is reflected in a recent industry report that forecasts four phases in the evolution of the mobile phone (Ask, 2012). In phase I the phone can be used to extract location, time-of-day and simple behaviour preferences that can then be passed to businesses or services in order to offer highly context specific products and services, tailored to the

[1] See http://girlsaround.me/. Accessed 3 December 2012

individual. In phase II, businesses should be able to combine the user profile with richer intelligence in order to deliver even smarter offers to the customer. In phase III, new sensor technologies embedded in the phone would deliver a multisensory capability that might, for example, involve the capacity to detect smell or alcohol on the breath. Finally, in phase IV, the incorporation of sensors coupled with voice and gesture control would develop the wand-like capability of the phone to point, capture, store and analyse objects in our ambient environment.

3.3 Affiliation to online social communities for the purposes of support, information and advice and the appropriation of personal experiences and opinions in decision-making, crowd-sourcing and sense-making (Social, Elective)

Individuals are drawn to like-minded communities and their subsequent behaviour will demonstrate community influence. Such things are well established offline, but are readily apparent online, where it becomes much easier to find like-minded others and to use those others as an information filter or sounding board. This is the process whereby isolated individuals are able to find information and support, but it is also the process whereby extremist groups are able to radicalise new recruits by drip-feeding a diet of highly polarised information and advice (Weimman, 2010).

Building on the sense of a personalised commercial service (which was discussed in the previous section in terms of consumer profiling), people can and commonly do elect to receive information that is specifically tailored to their interests and needs. Consider, for example, rightsidenews.com - a site which offers strictly conservative opinion on American politics and life, offering links to 'faith and family', 'the right to life' and 'freedom and guns'. Subscribers can, if they wish, select this site as their sole source of news, committing themselves fully to a right-wing worldview. But what are the consequences of such a choice? Parsell (2008) argues that the Internet promotes such narrowcast communities and that these in turn ferment prejudice and activism, resulting in social cleavage and community division.

Social networks are inevitably subject to biases of various kinds. Spiro *et al*. (2012), for example, analysed tweets made in the wake of the Deepwater Horizon oil spill and showed that people are much more likely to re-tweet messages containing explicit reference to hazard. While Mejova and Srinivasari's (2012) analysis of political messages demonstrated that, while Twitter is driven by news and is relatively lacking in any sentiment, YouTube is generally used as an outlet for opinionated speech.

With these findings in mind, should we be prepared to trust online information? We can explore this question by looking in more depth at one particular domain – health. While extremely polarised and dysfunctional health communities do exist online ('pro-anorexia' sites being a well-cited example), the transition to social media as the 'trusted' source of health information has been largely benign (e.g. Sillence *et al*., 2011). Shared patient experiences now form an important part of health decision-making: Fox (2011) reports for Pew Research Centre showed that 34% of internet users have drawn on such experiences and notes that chronic health sufferers are very likely to search online to connect with people facing similar health issues. Patient communities are therefore likely to be increasingly influential when it comes to individual health choices.

The deliberate use of an online community to answer a particular problem has become known as crowd-sourcing – and it is by no means limited to the health domain. Vast social networks can be used to seed specific problems or queries and the response from these networks can then be taken as some kind of ground-truth reflecting the 'wisdom of the crowd'. This opportunity can be coupled with the ability to mobilise crowds rapidly and effectively through tweets and messaging services. This relatively new ability – to shape the offline behaviour of an online community - begs the question: to what extent should the crowd or community be considered to have an 'identity' in its own right? Such questions are the focus of a new kind of study – web science – in which an online community is subject to data analytics of various types in order to define its characteristics (which can be made in terms of attributes such as personality, political opinion, communication style) and also to make predictions about the behaviour of that community (e.g. Kosinski *et al*., 2012; Rowe *et al*., 2012).

3.4 The use of reputation, rating and tagging systems as a means of public labelling (Social, Ascribed).

We are familiar with reputation systems (examples include eBay or ratemyteachers.com) that allow us to rate an individual or a business. We use reputation systems to both build and exploit online trust and social networks are increasingly providing this service. Brogin and Smith's 2009 bestseller 'Trust Agents: Using the Web to Build Influence, Improve Reputation, and Earn Trust' was a business demonstration of the effectiveness of social networking tools in this domain. Individuals now manage their social reputation from a very young age, using facebook tools, for example, to rate photographs of their friends ('Emily likes this') and then using these ratings as an aggregate measure of popularity.

In a number of phone-futures documents and videos, the idea that we might build and access these online reputations 'live' is gaining credence. This idea is premediated in science fiction movies where protagonists may wear glasses enhanced with face-recognition software that offers immediate access to personal profiles about the people they encounter (cf mission impossible IV). Here, fact is not far behind fiction: Samsung have already demonstrated a fully transparent display[2] and Apple seems to be following suit[3]. A transparent display is interesting, because it allows the combination of digital information with the objects or people in one's immediate view. An example (given by Apple) would be a tour bus fitted with smart windows that would augment real world views with informative descriptions. More immediately, the smartphone camera can be used to create a 'transparent' effect: Google Goggles[4] is an android app that allows the smartphone camera to access information about the objects in immediate view, but a more interesting 'identity' example is provided by Swedish firm TAT (The

[2] http://www.techspot.com/news/47058-samsung-demos-transparent-smart-window-prototype.html. Accessed 3 December 2012

[3] http://www.patentlyapple.com/patently-apple/2011/07/apple-developing-applications-for-smart-transparent-displays.html. Accessed 3 December 2012

[4] http://www.youtube.com/watch?v=8SdwVCUJ0QE. Accessed 3 December 2012

Astonishing Tribe), whose 'augmented ID' or 'Recognizr App' is described on their website: http://www.tat.se/videos/[5]. Essentially, this is a mobile phone application that captures the image of the person in front of you and uses face-recognition software in order to pull identity information about that person from the cloud, placing this profile data as an overlay on the original image. It offers the possibility of using the mobile phone as a means to scan the people around you in order to access public profiles in real time. In his novel 'Super Sad Sweet True Love Story', Gary Shteyngart (2010) describes a future in which such displays could be used to identify, say, the customers in a bar while simultaneously accessing their popularity, health and wealth ratings. This seems the more likely future for the bar – where individuals are pulling down contextual information to facilitate their social life in real time. Intriguingly, all of the technologies and social networks needed to achieve this are already here: facebook offers the opportunity for peer commentary and has recently acquired face-recognition software that would allow for such commentary to be accessed 'live' and Aquisti *et al* (2011) have shown that face-recognition software could be used to identify people on the basis of facebook photographs in order to extract 'confidential' personal data and make it public.

Another interesting means of accessing aspects of an individual's identity in real time was anticipated by Gasson and Warwick (2005), who suggested that the everyday objects we carry around with us may be RFID-tagged with identity information that could ultimately render us vulnerable. They imagine a future scenario in which personal valuables could be digitally recognised by would-be assailants who would have the capability to scan someone and infer their personal wealth, making on-the-spot judgments about the costs and benefits of robbing them.

[5] See http://www.tat.se/videos/. Accessed 3 December 2012

4. The machine as identity management agent

What is obvious about many of the developments cited above is that they entail an exchange of personal information on a vast scale. The need to monitor or even control information exchange on this scale has prompted the development of software agents that can act in a personal capacity to filter or manage information flow or that can extend influence. Ghanem *et al*. (2012) for example have explored interactions in social networks such as facebook in order to model the characteristics of those online identities that are most influential, while Koster *et al* (2012) have developed a means of allowing agents to reason about their mutual trust in each other. Such work heralds a future in which identity exchanges may be mediated by trust agents capable of facilitating or impeding interactions with unknown entities. Briggs and Olivier (2008) have suggested that trust agents could be implemented in companion devices bonded to an individual by physical and behavioural biometrics. These companion devices or 'biometric daemons' could then act, not only as the mechanism by which owners are authenticated (as they seek to access various services), but also as security advisors – signalling the likely threat associated with any new interaction. In a ubiquitous computing environment, for example, an individual may be bombarded with requests authorizing the release of personal data but may not be able to make individual decisions about the risks inherent in each request. A device with the capacity to monitor not only location or transaction information but the relationships between enquiring agents could become a kind of personal historian, maintaining and evaluating exchanges and ultimately assigning trust values to different enquirers.

The idea of an agent that somehow comes to represent one's personal values is found in Jane McGonigal's writing. In 2008, she employed a crowd-sourcing methodology at the Institute for the Future (IFTF) Technology Horizons conference, asking conference delegates to provide an answer to the following question: "In 2019, who defines your identities, and who governs them?" Answers are available in detail on her blog, but in aggregating the replies, she was most taken with the idea that some kind of intelligent agent or 'digital twin' could trawl through the dataspaces that we inhabit online and filter information on our behalf - effectively managing our online identities:

"these Digital Twins, these crudely-intelligent agents, are the primary 'filters' we will use to interact with the web, with complex objects of any type (our workspaces, our homes, our cars, our kitchens) and each other….The more that we use them, the better they get at protecting our values, advising us on wise ways to spend our money, and helping us use our votes to get more and more the kind of society we want."[6] Such a notion references a world in which our personal profiles - our 'digital twins' – rapidly become so complex that they can no longer be subject to interrogation on a human scale. This, then, defines a future in which, not only is an increasing element of our identity 'devolved' to machines, but in which machines – and machines alone – have the capability to process that identity.

[6] See http://www.iftf.org/node/2398. Accessed 3 December 2012

5. Implications

We have always known that identity is socially constructed, but one implication of the use of machines to do our identity work is that that this 'social construction' is recorded and may leave a trail of data artifacts that can be used by others. In two very real senses, we may 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. One major implication from this is that future technologies and services may be explicitly constructed to allow us to regain some of that control – offering, for example, visualisation services that allow us to understand our identity footprint, legal services that allow us to regain ownership of personal artifacts in the public domain; identity management services that give us executive control of our personal data; enhanced privacy services capable of filtering out personal, identifiable data from the public domain or even 'digital suicide' services (e.g. suicidemachine.org) that allow us to terminate our digital lives. We should note, however, that such developments are predicated on an assumption of the rights of the individual remaining paramount. There is an alternative, potentially longer-term vision, in which individual rights to digital ownership may be subsumed by the collective identity that is enabled by the Internet.

References

Aquisti, A., Gross, R. and Stutzman, F. (2011). Faces of Facebook: Privacy in the Age of Augmented Reality. Presentation to 4th Workshop on Security and Human Behaviour. *BlackHat USA,* 2011.

Ask, J. A. (2012). *The Future Of Mobile eBusiness Is Context*. May 1st 2012. Available from Forrester Research, http://www.forrester.com, accessed 18.6.12.

Briggs, P., & Olivier, P. L. (2008). Biometric daemons: authentication via electronic pets. Proc. *CHI 08 extended abstracts on Human factors in computing systems* (p. 2423–2432). ACM Press.

Brogin, C., & Smith, J. (2009). Trust Agents: Using the Web to Build Influence, Improve Reputation, and Earn Trust*. John Wiley & Sons publishers.*

Delaitre, S. (2006). Enjoy a Bar in 2012. Identity in a Networked World: Use Cases and Scenarios. Report from FIDIS: Future of Identity in the Information Society (No. 507512). Downloaded (14.6.2012) from: http://www.calt.insead.edu/project/Fidis/documents/2006-fidis-wp2-del2.6-Identity_in_a_networked_world.pdf

Fox, S. (2011). The social life of health information. Pew Internet & American Life Project Report, May 12, 2011. Available from Pew: http://pewinternet.org/Reports/2011/Social-Life-of-Health-Info.aspx*, accessed July 5th, 2012.*

Gasson, M. N., Kosta, E., Royer, D., Meints, M., & Warwick, K. (2011). Normality Mining: Privacy Implications of Behavioral Profiles Drawn From GPS Enabled Mobile Phones. *IEEE Transactions on Systems Man and Cybernetics Part C Applications and Reviews*, *41*(2), 251-261.

Gasson, M. and Warwick, K. (2005). Ubiquitous Computing Scenario. Report from FIDIS: Future of Identity in the Information Society (No. 507512). Downloaded (14.6.2012) from: http://www.fidis.net

Ghanem, A., Vedanarayanan, S. and Minai, A. (2012). Agents of Influence in Social Networks. *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012),* Conitzer,Winikoff, Padgham, and van der Hoek (eds.), 4-8 June 2012, Valencia, Spain.

Gulotta, R., Faste, H., & Mankoff, J. (2012). Curation, provocation, and digital identity. *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems CHI 12* (p. 387). ACM Press

Joinson, A.N., Houghton, D., Vasalou, A., Marder, B. (2011). Digital Crowding: Privacy, Self-disclosure and Technology. In S.Trepte & L.Reinecke (Eds), Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web (pp 31-44). Springer, Heildelberg & New York.

Kirk, D. S., & Sellen, A. (2010). On human remains. *ACM Transactions on Computer-Human Interaction*, *17*(3), 1-43. ACM.

Kosinski, M., Bachrach, Y, Kasneci, G, Van-Gael, J and Graepel, T. (2012). Crowd IQ: Measuring the Intelligence of Crowdsourcing Platforms, Proceedings of Web Science 2012, ACM Press, 45-54.

Koster, A., Sabater_Mirhas, J. Shorlemmer, M. (2012). Personalising Communication about Trust. *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012),* Conitzer,Winikoff, Padgham, and van der Hoek (eds.), 4-8 June 2012, Valencia, Spain.

Martin, T. (2012). Placeme is the future of mobile services. Available from phonedog.com (http://www.phonedog.com/2012/04/12/placeme-is-the-future-of-location-based-services/), accessed 3.7.12.

Mejova, Y. And Srinivasari, P. (2012). Political Speech in Social Media Streams: YouTube Comments and Twitter Posts. Proceedings of Web Science 2012, ACM Press, 307-310.

Odom, W., Sellen, A., Harper, R and Thereska E. (2012). Lost in Translation: Understanding the possession of digital things in the cloud. Proc. CHI 2012, ACM Press.

Parsell, M. (2008), Pernicious Virtual Communities: Identity, Polarization and the Web 2.0. Ethics and Information Technology, 10:1, 42-56.

Rowe, M., Fernandez, M, Alani, H., Ronen, I, Hayes, C. And Karnestedt, M. (2012). Behaviour analysis across different types of Enterprise Online Communities. Proceedings of Web Science 2012, ACM Press, 387-396.

Shteyngart, G. (2010). Super Sad True Love Story. Random House.

Sillence, L., Mo, P., Briggs, P., & Harris, P. R. (2011). The Changing Face of Trust in Health Websites. *Phoenix USA*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1920317

Spiro, E., Sutton, J. Greczek, M, Fitzhugh, S., Pierski, N. And Butts, C. (2012). Rumoring During Extreme Events: A Case Study of Deepwater Horizon 2010. Proceedings of Web Science 2012, ACM Press, 418-426.

Weimann G. (2010) Terror on Facebook, Twitter and Youtube. *Brown Journal of World Affairs*, 16(2), 45-54.

Zaslow, J. (2002). If TiVo Thinks You Are Gay, Here's How to Set It Straight. *Wall St. Journal*, November 26th, http://online.wsj.com/article_email/SB1038261936872356908.html. Accessed, 28.6.2012.

Acknowledgement

The author would like to acknowledge collaborators from the EPSRC-funded IMPRINTS project (http://www.imprintsfutures.org/) who were helpful in capturing many of the identity futures outlined in this review.

Foresight
1 Victoria Street
London SW1H 0ET
www.foresight.gov.uk
URN 13/506