Exercising identity: agency and narrative in identity management

Liesbet Van Zoonen and Georgina Turner
Department of Social Sciences, Loughborough University, Loughborough, UK

Abstract

Purpose – The purpose of this paper is to address the paradox in identity management that sees people happily sharing personal information in some circumstances, such as via social networks, yet defending their right to privacy in others, such as in interactions with the state. The authors examine the predominant explanations and elaborate how these ignore the different types of individual acts and agency involved in identity management. The authors conclude with a proposal to consider alternative, narrative approaches to identity management (IM).

Design/methodology/approach – This paper has been developed out of the empirical research examining public responses to new forms of IM, based on, among other things, Delphi interviews with experts, films and television series and survey and focus group data about people's feelings and attitudes. The authors have combined these data into an approach that theorises rather than reports about public engagements with IM.

Findings – Finding any explanation for the paradox that rests on the distinction between state and commercial contexts to be less and less satisfactory, the paper reframes the problem as one of varying degrees of agency, from submission to transaction and expression. The latter, the authors argue, has been written out of modern IM, which is at odds with the centrality of narrative to the human sense of self.

Originality/value – The field of IM has yet to consider "identity" in terms beyond distinct attributes and bits of information. In this paper the authors set out to demonstrate the value of a notion of IM that is sensitive to degrees of agency and the authors ask how the fundamental human desire to narrate the self might become a part of IM systems.

Keywords Cross-cultural studies, Identity, Privacy, Agency, Citizenship, Technology acceptance, Authentication, Authority, Biometrics, Narratives, Identity management technologies

Paper type Conceptual paper

When we consider the ways that people manage their identities – specifically, how they prefer to manage their identities in particular contexts – we find a noticeable paradox: people are happy to share personal information about themselves (and their families) on social media such as Facebook, yet are resistant to providing information that would facilitate, for instance, electronic patient files in the health service. They will give their personal details readily in order to obtain a customer loyalty card (on an average the UK's major schemes[1] have 16.7 million active users, though in some cases application forms for this type of card can run to more than ten pages), yet are moved to protest against a national identity card. A 2013 survey found that this paradox is most notable in the USA and the UK, two countries recently shocked by revelations of clandestine government surveillance and data-mining. Nevertheless, 88 per cent of the USA and 69 per cent of the UK population feel happy to share their personal details with retailers[2].

Often this paradox has been explained by the distinction between commercial and government contexts, with commercial interactions being perceived as voluntary and beneficial rather than an obligation to the state. This distinction came up repeatedly, for instance, in the Delphi interviews we conducted with UK experts on

identity management (IM) from various fields[3]: "[Loyalty card holders] get discounts. You get sent tokens based on your shopping, which give you money off future purchases. There is a very clear benefit. The government has offered no pay-off for ID cards; they have simply said, 'you are going to have to do this'".

The distinction between commercial and government contexts has also been clearly visible in public discourses on topics such as identity cards, security and surveillance and biometric technologies, which often refer to the work of George Orwell; developments in technology are frequently framed in terms of (inexorable) moves towards the dystopian world of Nineteen Eighty Four. There is a discernible tendency, particularly in news coverage of such technological developments, to use particular films and television series as examples of what the future of IM could look like (Turner et al., 2014), but the prevalence of Orwell prescribes an emphasis on risk over opportunity, on fear over desire, and it relates primarily to those developments stemming from government. The recent revelations about the covert surveillance programmes in the USA and the UK are a case in point: so frequent were the references to Nineteen Eighty Four as the news of Prism broke that sales of the book on Amazon increased by 7,000 per cent[4].

There is good reason to suggest that public concerns about IM depend upon who is asking for identity data: while fingerprinting in schools (to administer cashless canteens, for instance) is an "Orwellian" system akin to "Big Brother" according to the Guardian[5], the news that the next iPhone will feature a fingerprint scanner is greeted with excitement: "how cool would that be?"[6] One of the journalists participating in our Delphi interviews said: "We certainly have created an atmosphere in which government is seen as something to be afraid of […] the media have contributed to a climate in which government is the villain. It's not just the news media, I'm thinking of Hollywood; it's a safe plotline to have in any drama, or even comedy programmes".

The distinction between governments and commercial institutions, however, offers a limited and decreasingly satisfactory explanation for the main paradox of IM, i.e. that people simultaneously value privacy and enjoy public self-disclosure. Such lack of explanatory value is highlighted by the shift in public discourse around Facebook, for example, which is increasingly centred around privacy concerns: of 1,488 UK news articles to include the search terms "Facebook" and "privacy concerns", 525 (35 per cent) were published in the year to April 2013[7]. This trend suggests that in the public imagination, Facebook is no longer a benign mechanism for sharing with friends and family; it has joined Google and various other corporate players in posing a threat to our personal data (particularly since Prism relied on major technology companies, including Facebook). In addition, in on-screen dramatisations, we see increasing numbers of plots in which commercial interests, rather than governments, fill the role of the bad guys: for instance in the 2011 web series H+, featuring an unscrupulous biotechnology company; in the 2012 BBC television series Hunted, in which a consortium of five major multinational corporations conspire for power; and in the ongoing Canadian science fiction series Continuum, imagining a future in which governments have been replaced by all-powerful corporations. This is not a world of high-tech opportunity but of such complete dystopia that protestors travel back in time, to 2012, to alert the developed world to what it is creating for the future.

Looking more closely at acts and agency in IM
The notions of commercial vs state interaction, and voluntary vs obligatory disclosure, are thus becoming less adequate to explain the play between the desire for privacy and

the appeal of self-disclosure and sharing. We propose that in order to understand the paradox, a different concept of identity is needed than is currently used in the field of IM, where identity is considered to be the sum of different units of information about a human being: date of birth, for example; a number assigned by a government such as a national insurance number; a biometric feature and so on. Any combination of such pieces of information that delivers a 100 per cent certainty in establishing who somebody is, what his or her needs are (in commercial tracking) and what kinds of risks s/he produces for national security, is an identity manager's dream.

Such approaches take identity to be a measurable set of features that, once established, will define a person and enable authentication across time and space. The requirements for passport pictures imposed on its citizens by the UK government are a case in point. The image of you, says the Gov.uk web site[8], "should show a close-up of your full head and shoulders. It must be only of you *with no other objects or people*" (our italics). Evidently, according to this part of the rules, you are not defined by others or things, and your most important part is your head. Furthermore, the UK government wants you photographed, "facing forward and looking straight at the camera; with a neutral expression and your mouth closed; without anything covering the face; without a head covering (unless it's worn for religious or medical reasons); with eyes open, visible and free from reflection or glare from glasses; with your eyes not covered by sunglasses, tinted glasses, glasses frames or hair". The resulting picture is unlikely to be recognised or acknowledged by the person as a picture of "me". The "being" that is in the picture is certainly a different one to the "being" people have constructed for themselves.

The gap between the official passport representation and a person's sense of self is about more than appearance and looking good in a picture. It opens up consideration of another paradigm of identity not only as something that we are, but also as something that we do. It is apparent that a certain presentation of self, in Goffman's (1959) terms, is always involved in one's identity, which thus involves doing in addition to being. It is this doing of identity that is ignored in the quickly emerging field of IM, defined as the identification and authentication of individuals *vis-à-vis* other people, organisations and increasingly their things[9]. In fact, we can go so far as to suggest that it is the business of IM to ignore and elide such narrative and performative identities. Attributes can be measured and catalogued, re-identified – and re-identified at a distance, even without the knowledge or approval of the subject, who is thus rendered the object and deprived of selfhood. Ajana (2010, p. 18) calls this "the failure and the dream of the biometrics". We would argue that the failure of modern IM is a failure to take into account the resilience, the relentlessness, of the need to build the self not from distinct constituent parts but through a life story about oneself; biography, or narrative identity. The paradox that sees concerns about privacy co-exist with self-disclosure, then, is not (only or primarily) borne of the distinction between commercial- and state-driven IM, but of the distinction between the administration of information, and the opportunity to tell one's own story, to express oneself. The issue is one of agency. It is clear that different "moments" of and for IM involve different kinds of acts and allow different degrees of freedom *vis-à-vis* the institution requesting identification or authentication. Though these different kinds of acts can be said to exist as points on a spectrum rather than as discreet categories, we suggest that to show your papers is an act of submission to the state; to enter your pincode at the ATM, or enter your password for online banking or shopping, involves a transaction in which you get something back; to share your personal details on Facebook is an act of self-expression

(although radical thinkers would claim that it is an act of submission to capitalism or peer pressure).

Acts of submission

In acts of submission the central operating mechanism is coercion, where some kind of leverage is used to elicit compliance – though other mechanisms may also be at work, albeit in some smaller way. For instance, if a police officer stops you in your car and asks you to identify yourself, you have little choice but to show some kind of ID. Such coercive "moments" involve unequal power relations, though this does not mean that acts of submission are inevitable: citizens must acknowledge the authority of the state, or its law enforcement, and consider the request for information to be legitimate.

Neither the state's authority nor (and especially) the demand's legitimacy is stable and self-evident – in fact, both seem routinely to be up for question. In 2009, the British government abandoned plans for compulsory identity cards in the face of public campaigning and increasingly derisory media discussions. Police powers to stop and search face regular scrutiny in much of the UK press, and in 2012 developers created a mobile phone app to enable those stopped to log the details of the encounter and record their evaluation of it, creating a public database of police behaviour to mirror police records themselves[10].

This is an ongoing power tussle, and whether state requests for identification will be experienced as an act of submission is susceptible to significant flux. Shortly after 9/11, Westin (2003) found strong support for new and more invasive investigative powers for the US government, even as respondents expressed concerns about their proper use. A year after the attacks, however, support for some measures, such as the monitoring of internet discussions, e-mails and mobile phones, had dropped by as much as 22 per cent (p. 448). In research conducted several years later, Sanquist *et al.* (2008) find that measures such as e-mail monitoring are likely to elicit the strongest negative reactions, lending further credence to the assertion of a relationship between a sense of imminent danger and public willingness to submit to the state, and the waning of that willingness "as memories of threats fade" (Sanquist *et al.* (2008), p. 1126; see also Davis and Silver, 2004; Waldron, 2003)[11]. Thus, we see perceptions of IM as acts of submission change in the wake of major events: anti surveillance powers as the whistle is blown on Prism; pro surveillance within hours of the murder of a British soldier by Islamic extremists[12].

The authority of the state must be acquired again and again: though he says postwar governments enjoyed relatively high levels of public trust and confidence, Hajer (2003) points out that "trust was never simply there and [...] needed to be reconfirmed constantly" (p. 184). Now, when security breaches and data losses – from laptops left on trains to sensitive e-mails sent to the wrong address – have tarnished successive US and UK governments[13], only distrust can be assumed. Trust, or some acceptable consensus of trust, must be won for each new occasion in an iterative process that sits counter to any identity measure that demands a single and final submission to authority. "Even carrying a government-issued ID is a very contentious issue here", said one of our US experts in the Delphi interviews. "People would totally freak out. They think, 'something bad will happen to me if people know who I am'. It's a nebulous concern [...] a primal fear".

In this context we must wonder if IM that requires an act of submission (and only an act of submission), or is perceived as such, can ever be adequate – is coercion sufficient, let alone desirable? "An identity card is like being told that I've got to wear an identity

bracelet, or some kind of tag, which we kind of think of as referring to criminals", said one expert in the Delphi interviews. Addressing the fact that people are happy to sign up for store cards, another said: "The government has offered no pay off for the ID cards. They have simply said, 'you are going to have to do this and it's going to be a bit tedious […] and the benefit is the rather indistinct one of reducing terrorism and crime'. People look at that and they say, 'that's not a very good trade off'. They look at loyalty cards and they see a good trade off. Good trade offs win and bad trade offs don't". The suggestion that people desire something in return for offering their personal data brings us to IM as acts of transaction.

Acts of transaction

In this category we include those acts that involve some kind of exchange. Most involve individuals choosing to provide an institution or organisation with their personal data in a "swap" for rights (e.g. in exchange for your personal information, a bank may lend you money). In the case of membership/store cards, personal information (and permission to build lucrative data on shopping habits) is exchanged for entitlement to offers and discounts. Some involve a peer-to-peer exchange, between individuals or groups of individuals, as in the case of collaborative consumption schemes such as Airbnb (where users can rent spare rooms from other users), ZipCar (where users share access to cars stationed in their city) and Zopa (where individual lenders contribute to cash loans for other users).

Where coercion is the main mechanism in acts of submission, trust is the crucial element in transactions. Trust must be mutual and both parties – the identifier and the identified – assume some level of equivalence: the value of the information given up is at least equivalent to the value of the goods, services or rights offered in return. Importantly, this is a subjective judgment; those who consider their information to be more valuable than the entitlements/discounts/cheap accommodation on offer are under no obligation to partake.

Examples of trust being abused are plenty: Craigs list has been associated with numerous "scams", including users who take deposits for letting a house that in fact they do not own; one Airbnb scammer is so well known that there are online support group for his victims[14]; there are enough eBay scams around to merit top ten lists[15]. It is not only in peer-to-peer transactions, either: in 2012 a couple were jailed after using 1,400 false identities to claim millions of pounds in benefits from HMRC[16]; a year earlier an IT manager at Sainsburys was jailed for setting up multiple Nectar (reward) accounts and adding thousands of points. There was disgruntlement in 2013 at the news that Tesco planned to use Clubcard data to monitor customers' diets and suggest healthier options, as well as passing on information to be used in government research in to obesity[17].

Such security breaches and fraud cases are among the reasons why members of the public are wary of providing personal information. Our survey and focus group data show a strong concern about identity fraud, and a considerable desire for greater control over one's personal data (see Van Zoonen and Turner, 2013). We have shown elsewhere how these fears exist in a cultural and media context which has a tendency to envisage a dystopian Orwellian future in which the state exercises invasive levels of control over their citizens' identities (see Turner *et al.*, 2014). In USA and UK productions such as Gattaca (1997), Enemy of the State (1998), Minority Report (2002) or The Last Enemy (2008) the arm of the state is not only long but it also has a vicious and indiscriminate grip. The recent emergence of commercial "baddies" in

pop culture – The Hunger Games, Hunted and Continuum (all 2012), for example, as well as titles such as Unknown, In Time, Black Mirror and H + (all 2011) – may further exacerbate this climate of fear around the risks of identity transactions, regardless of whom exactly you share your date with. The literature addressing (the future of) IM has tended to focus on the perceived trade off between data required and service rendered – see Camenisch *et al.* (2011). As we will elaborate in the next section, this only explains a part of the paradox.

Acts of expression

When we consider identity merely in terms of submission enforced by coercion, or as transactions based on trust, we abide by a logic similar to the one at work in more general ideas around technology acceptance (cf. Davis, 1989): we assume, to a greater or lesser degree, that consumer-citizens are rational actors who decide on the basis of knowledge (or perception) of necessity, usefulness, ease of use, risks, benefits and so on. Where we see contradictions in those decisions – as, say, in the case of a Facebook user who campaigns against a national ID card – we might seek to explain them by reference to other influential factors, such as perceptions of the identifying entity (and, as above, then to popular cultural representations).

What if instead, we set aside the assumption that users behave as rational actors? What if we cross the divide that separates this sort of identity work, where identity is a matter of information management, from work that has identity as a matter of self-expression? Sociocultural approaches to identity have for a long time concerned themselves with dramaturgy (cf. Goffman, 1959) and performativity (cf. Butler, 1990); with the doing of identity. People are not the sum of a set of measurable, quantifiable attributes and neither are they completely rational actors. They are also the product of the iterative and narrative performances of the person they consider themselves to be.

Ricoeur (1990) differentiated two aspects of identity: the *Idem* being those attributes that remain, or are assumed to remain, constant, and the *ipse* being the sense of self, the biographical narrative that we (re)tell about ourselves throughout our lives. It is the *Idem* that has, "naturally", become the focus of IM; IM is often a question of re-identification, to which the reliability, the apparent sameness of particular categories and characteristics, holds an appeal that the shifting, unstable narrative of a life lived cannot. As Ajana (2010, p. 246) suggests, the aspirations of biometric technologies are at odds with narrative – they seek to circumvent narrative, "finding recourse in the body itself and turning it in to a stabiliser of identity".

If we look at studies such as Sehulster (2001) and Vonèche (2001), which show the variation and elaboration in people's (re)tellings of their own stories, we can see the grounds for administrative suspicion of narrative identities – yet, simultaneously, we can recognise the fiction of a single identity that is the sum of distinct units of data. We can also see that people like to tell stories about themselves; their sense of self may at times and in specific contexts be coloured by certain (bodily) characteristics, but people are authors of self, and it is through these stories that they see themselves as most unique. When people share their personal information on Facebook, or Twitter, or Tumblr, they are not simply handing over dividuated fragments of information. They are narrating their lives, performing a self for public consumption; we see our friends and families share photos of beautiful views, news of significant achievements and intimate moments. In some sense, social media technologies have enabled us to return to pre-modern instruments of identification.

As most authors in this field have identified, the need for identification and authentication emerged with modernity and the nation-state. In the small, local communities of previous times people knew each other and their direct authorities. In the unlikely event that they had to leave their vicinity, a set of cultural markers would identify the groups to which they belonged (e.g. nobility, clergy, merchants, peasants), giving them access to members of the same group at their destination. Criminals in some areas would be physically marked for future identification (Cole, 2001), and members of guilds could prove their status through their specialised knowledge or symbols of their craft (see Rode, 1989). The ordinary person, though, had little else than his or her life history to identify them, and the truth of that story was assessed only on the basis of its credibility and affirmation by others. The well-documented case of Martin Guerre, an imposter in the French countryside of the sixteenth century, shows us two things in this respect. First, that such a narrative identity could be easily set up but was difficult to assess. As Cole (2001, p. 6) says about the trial of the imposter, the court relied heavily on "tests of memory, evaluations of dialect and the confused and divided recollections of eyewitnesses"[18]. Second, the Martin Guerre case demonstrates profound and permanent collective anxieties about identity. In her seminal analysis of the episode, Nathalie Zemon Davis (1983) traces an immediate "news" flow around the court case, circulating "like other 'terrible' and 'marvelous' cases of murder, adultery, fire and blood" (p. 104). Stories about identity deception have been, in fact, a staple ingredient of Western culture dating back to Greek mythology, which is abundant with Gods posing as animals before abducting, abusing and exploiting people, women in particular (see Murnaghan, 2011) – a trope that, interestingly, is currently heavily repeated in the panics about "stranger danger" on the internet (e.g. Van Zoonen, 2011).

Small wonder that a better means of identification became a societal necessity when industrialisation and urbanisation produced unprecedented flows of people setting off to unknown places, a continuous coming together of strangers. There was a staggering rise in swindling and fraud made possible by the new anonymity of the urban crowds (Cole, 2001). As an expression of the anxieties brought about by modernity, the crime and detective novel rapidly gained popularity, as did stories of multiple and suspect identities like that of Dr Jekyll and Mr Hyde (cf. Boltanski, 2011). In real life, photography, fingerprinting and the passport were nineteenth century answers to the challenges of massive mobility, underpinned by both technological and epistemological innovations. These enabled the objective identification of bodily features as the core to one's identity, especially in combination with authoritative tokens like the passport. This combination remained the main paradigm for identification until the emergence of automated banking and, later, the internet introduced memory-based authenticators such as pincodes and passwords.

The current time, then, is one in which identification and authentication are based on a bodily feature, a code one remembers, or a token one possesses. From the perspective of government and society this has made for the most trustworthy (available) system, but from the perspective of the individual it is fundamentally flawed. Numerous are the anecdotes of forgotten passwords, mistyped pincodes and lost credit cards as examples of human fallibility; of identity theft and hacked accounts as evidence of human wrongdoing; of misinterpreted fingerprints and DNA (for the latter see McKie and Russell, 2007) as evidence of human error. More fundamentally, however, the current paradigm denies that a crucial and undeniable element of human identity is narrative.

This is not a new idea, but one that has been – elsewhere – (re)discovered. In psychology, for instance, McAdams (1995) developed the concept of narrative identity, suggesting that an individual is not simply a mass of (psychological) traits and concerns but is also in need of a sense of coherence and purpose, which is constructed in and of one's life story. People's desire to tell their stories is evident, and while private life has always provided forums for such storytelling (Langellier and Peterson, 2006), we now see increasingly numerous public forums, too. On television, "subjective, autobiographical and confessional modes of expression […] proliferated during the 1990s" according to Dovey (2000, p. 1), who also alludes to an increasing and wider cultural relevance of the confessional mode. Social networks such as Facebook and Twitter now furnish people with the tools to tell stories big and small to far larger audiences: at the start of 2014, Twitter has 241 million active users[19], Facebook 1.23 billion[20]. Narrative is insuppressible. If people's unique sense of self is bound up in the stories they tell – and if they are happier telling those stories, being rather than identifying themselves – can IM technologies work with, rather than against, that?

Discussion: possibilities for narrative IM?

We have set out the paradox in contemporary IM that sees people happy to share information in certain contexts but angrily defending their right to anonymity in others. While this paradox has previously been (and can still in part be) explained by the difference between our feelings about dealings with corporations and peers and dealings with state bodies, we have attempted to reframe the problem less as one of whom we are dealing with, and more as what it is that we are asked to do; in other words, as an issue of agency. Specifically, we consider the act of self-expression and its omission from modern IM systems. While this omission has been deliberate – in deference to the apparent reliability and replicability of biometric and/or token measures – it is at odds with the resilient centrality of narrative and performance to the human sense of self. Organisations may wish to ignore self-expression, but it is unlikely to go away. In fact, there is evidence to suggest that the more that self-expression is written out of IM, the more some people will buck against the system. In 2008, for instance, Transport for London warned that users who melted their Oyster cards to retrieve the RFID chip and attach it to their watches (thus enabling them to enter the transport system with a casual swipe of the wrist) faced fines[21], a threat that it was forced to reiterate when Jamie Whitby, the "urban wizard", built the chip in to a magic wand three years later[22]. In response to the fact that only religious headgear was permitted in photographs for Austrian driving licences, one driver in 2011 insisted on wearing a colander on his head, to symbolise his "pastafarian" beliefs[23]. Alongside the development of new surveillance technologies have come the means to play with and resist them (using, for instance, cosmetic and visual designs that make automated recognition impossible[24]).

People cannot conceive of themselves as a data set, or as someone who will not (must not) change over time. Our argument, then, is that any system of IM that involves human beings ought, if it is to be widely, willingly and properly used, to allow those human beings to exercise their identity or identities over the course of a lifetime. While thus we may have resolved the privacy/self-disclosure paradox, we knowingly raise additional questions for IM. Is there a way to combine narrative identity with efficient and trustworthy systems? We have already seen some moves in this direction – a number of online interactions now require not only a username and password, but also the answer to personal questions: what street did you grow up on?

What was the last school you went to? What was the name of your first pet? Standing alone the answers may stretch the definition of narration, but the process of answering is a narrative one. During the London Olympics, Oyster card users were offered covers showing their national flags, enabling the expression of one's (national) identity in the London subway. In 2013 Barclays bank began advertising personalised (with a chosen photo) debit cards[25], again suggesting a move towards self-expression in IM.

While these are somewhat cosmetic (but not unimportant) changes, the currently evolving practices of lifelogging may offer more fundamental shifts for narrative identification. O'Hara *et al.* (2008) argue that lifelogging, and by extension a collection of (say, Facebook) status and location updates, can be empowering to the individual in different ways, and provides narrative means of identity construction that can be helpful in interactions with governments and corporate partners. Lifelogging, they argue, would protect those regularly and incorrectly suspected of terrorist activity (for, e.g. see Coughlin, 2007, as cited by these authors); would offer opportunities for "sousveillance" (watching the watchers); and would make it more difficult for authorities to impose identities on subjects. As they conclude: "the lifelog, for the lifelogger, might constitute the 'real' person" (p. 21) better than an ID card or passport. Importantly, the lifelogger keeps control over his or her own data, in stark contrast to the emerging popularity of behavior-metrics in which individual consumer behaviour is measured and analysed by external institutions and authorities.

While a narrative dimension in systems of IM may articulate a fundamental human desire, it also carries risks and exclusions of its own. Particularly as some – in an ageing population ever more – people are not capable of telling stories about themselves because of cognitive or memory dysfunction; for Alzheimer patients a question about the street they grew up in could be problematic. For them, body based means of identification or even RFID implants may be more desirable (see e.g. Wagemakers *et al.*, 2014). Evidently there are also risks and deep cultural fears about fabricated and false life stories, as our short digressions into history and popular culture demonstrated, and as is apparent in current fears about stranger dangers and identity fraud. Our point, therefore, is not to replace the current information-based paradigm for IM with a narrative one. Rather, we suggest that systems of IM which do not or cannot take into account the narrative desires of individuals, whether in their role of citizen, consumer or significant-other, are less likely to be accepted, let alone embraced, than ones that do offer the opportunity to exercise and express identity.

Notes

1. Tesco Clubcard, Nectar and Boots Advantage card.

2. Taken from www.businessweek.com/articles/2013-06-25/privacy-paradox-americans-happy-to-share-personal-data-with-big-business

3. We are currently conducting a Delphi study among experts in identity management, see for more detail: www.imprintsfutures.org/identity-management-in-the-future-imagining-2025/

4. www.theguardian.com/books/booksblog/2013/jun/11/george-orwell-prism-big-brother-1984

5. "School surveillance: how big brother spies on pupils", *Guardian*, 9 June 2011.

6. "The next iPhone's killer feature? Fingerprint scanning", www.idownloadblog.com/2013/04/12/iphone-5s-exclusive-feature-fingerprint-scanning/ (accessed 29 April 2013).

7. The search was done using the Nexis database. In each of the previous four years, an average of 217 articles matching these criteria were published. This means that fewer than 100 articles mentioned privacy concerns before 2008, though British broadsheets began reporting on Facebook in late 2005 (tabloids typically followed suit a bit later). Facebook was opened up to anyone above the age of 13 in September 2006, and by August 2008 had 100 million active users.

8. www.gov.uk/photos-for-passports

9. In a cultural and psychological understanding of identity management as being about the way individuals feel and interact, this notion of doing identity is much more manifest.

10. www.guardian.co.uk/law/2012/jun/15/stop-search-app-rights-police

11. The change in public mood has also been put down to media coverage that subsequently revealed the extent to which 'ordinary people' were being surveilled (Mariner, 2007).

12. www.guardian.co.uk/uk/2013/may/23/woolwich-latest-developments-live#block-519e2babe4b0e392888614fa

13. www.thebureauinvestigates.com/2012/05/23/is-your-data-safe-government-departments-plagued-by-data-losses/

14. www/fodors.com/community/europe/airbnbscam.cfm

15. http://google.co.uk/search?q = top + 10 + ebay + scams

16. http://metro.co.uk/2012/09/28/adeola-thomas-jailed-for-3-8m-benefit-fraud-using-1400-identities-589011/

17. www.dailymail.co.uk/news/article-2331856/Tesco-use-Clubcard-data-eating-what.html

18. Cole takes his information from Zemon Davis (1983).

19. www.reuters.com/article/2014/02/05/us-twitter-results-idUSBREA141ZZ20140205

20. http://theguardian.com/technology/2014/feb/04/facebook-10-years-mark-zuckerberg

21. http://london-underground.blogspot.co.uk/2008/08/oyster-watches-could-get-you-fined.html

22. http://jamiewhitby.com/urban-wizard/

23. www.bbc.co.uk/news/world-europe-14135523

24. The designer Adam Harvey has been particularly active in this regard: www.guardian.co.uk/artanddesign/2013/mar/31/anti-drone-hoodie-big-brother

25. www.barclays.co.uk/PersonalisedDebitCard/BarclaysPersonalisedCard/P1242605602883

References

Ajana, B. (2010), "Recombinant identities: biometrics and narrative bioethics", *Journal of Bioethical Inquiry*, Vol. 7 No. 2, pp. 237-258.

Boltanski, L. (2011), *Enigmes et complots : Une enquête à propos d'enquêtes*, Gallimard, Paris.

Butler, J. (1990), *Gender Trouble*, Routledge, London/New York, NY.

Camenisch, J., Fischer-Hübner, S. and Rannenberg, K. (Eds) (2011), *Privacy and Identity Management for Life*, Springer Press, New York, NY/Heidelberg.

Cole, S. (2001), *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard University Press, Cambridge, MA.

Coughlin, K. (2007), "Tracking himself, so the FBI won't have to", available at: http://blog.nj.com/digitallife/2007/10/tracking_himself_so_the_fbi_wo.html (accessed 28 June 2013).

Davis, F.D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *MIS Quarterly*, Vol. 13 No. 3, pp. 319-339.

Davis, D.W. and Silver, B.D. (2004), "Civil liberties vs. security: public opinion in the context of the terrorist attacks on America", *American Journal of Political Science*, Vol. 48 No. 1, pp. 28-46.

Dovey, J. (2000), *Freak Show: First Person Media and Factual Television*, Pluto Press, London.

Goffman, E. (1959), *The Presentation of Self in Everyday Life*, Penguin, London.

Hajer, M. (2003), "Policy without polity? Policy analysis and the institutional void", *Policy Sciences*, Vol. 36 No. 2, pp. 175-195.

Langellier, K.M. and Peterson, E.E. (2006), "Narrative performance theory: telling stories, doing family", in Braithwaite, D.O. and Baxter, L.A. (Eds), *Engaging Theories in Family Communication: Multiple Perspectives*, Sage, Thousand Oaks, CA, pp. 99-114.

McAdams, D.P. (1995), "What do we know when we know a person?", *Journal of personality*, Vol. 63 No. 3, pp. 365-396.

McKie, I. and Russell, M. (2007), *Shirley McKie: The Price of Innocence*, Birlinn Ltd, Edinburgh.

Mariner, W.K. (2007), "Mission creep: public health surveillance and medical privacy", *BUL Review*, Vol. 87 No. 2, pp. 347-395.

Murnaghan, S. (2011), *Disguise and Recognition in the Odyssey*, Lexington Books, Lanham, MD.

O'Hara, K., Tuffield, M. and Shadbolt, N. (2008), "Lifelogging: issues of identity and privacy with memories for life", paper presented at Identity and the Information Society, 28-30 May, Arona, available at: http://eprints.soton.ac.uk/265993/1/oharaet_al_idis_lifelogging.pdf (accessed 28 June 2013).

Ricoeur, P. (1990), *Oneself as Another*, University of Chicago Press, Chicago, IL.

Rode, M.W. (1989), "The nursing pin: symbol of 1,000 years of service", *Nursing Forum*, Vol. 24 No. 1, pp. 15-17.

Sanquist, T.F., Mahy, H. and Morris, F. (2008), "An exploratory risk perception study of attitudes toward homeland security systems", *Risk Analysis*, Vol. 24 No. 4, pp. 1125-1133.

Sehulster, J.R. (2001), "Richard Wagner's creative vision at La Spezia, or, the retrospective interpretation of experience in autobiographical memory as a function of an emerging identity", in Brockmeier, J. and Carbaugh, D. (Eds), *Narrative and Identity: Studies in Autobiography, Self and Culture*, John Benjamins, Amsterdam, pp. 187-218.

Van Zoonen, L. (2011), "The rise and fall of online feminism", in Christensen, M., Jansson, A. and Christensen, C. (Eds), *Online Territories: Globilization, Mediated Practice and Social Space*, Peter Lang Publishers, Oxford, pp. 132-147.

Van Zoonen, L. and Turner, G. (2013), "Taboos and desires of the UK public for identity management in the future: findings from two survey games", *Proceedings of the 2013 ACM Workshop on Digital Identity Management*, ACM, pp. 37-44.

van Zoonen, L., Turner, G. and Harvey, J. (2014), "Confusion, control and comfort: premediating identity management in film and television", *Information, Communication and Society*, available at: http:dx.doi: 10.1080/1369118X.2013.870592

Vonèche, J. (2001), "Identity and narrative in Piaget's autobiographies", in Brockmeier, J. and Carbaugh, D. (Eds), *Narrative and Identity: Studies in Autobiography, Self and Culture*, John Benjamins, Amsterdam, pp. 219-246.

Wagemakers, S., van Zoonen, L. and Turner, G. (2014), "Giving meaning to a RFID or cochlear implant", *Technology and Society Magazine, IEEE*, Vol. 33 No. 2, pp. 73-80.

Waldron, J. (2003), "Security and liberty: the image of balance", *Journal of Political Philosophy*, Vol. 11 No. 2, pp. 191-210.

Westin, A.F. (2003), "Social and political dimensions of privacy", *Journal of Social Issues*, Vol. 59 No. 2, pp. 431-453.

Zemon Davis, N. (1983), *The Return of Martin Guerre*, Harvard University Press, Cambridge, MA.

Further reading

Crapanzano, V. (2004), *Imaginative Horizons: An Essay in Literary-Philosophical Anthropology*, University of Chicago Press, Chicago, IL.

Dempsey, J.X. and Rosenzweig, P. (2004), "Technologies that can protect privacy as information is shared to combat terrorism", *Legal Memorandum*, Vol. 11, May, pp. 1-12.

Koslosky, D. and Baldwin, F. (2012), "Mission creep in national security law", *West Virginia Law Review*, Vol. 114 No. 2, pp. 669-724.

McAlpine, M. (2005), "E-portfolios and digital identity: some issues for discussion", *E-Learning and Digital Media*, Vol. 2 No. 4, pp. 378-387.

About the authors

Liesbet Van Zoonen is a Professor of Communication and Media Studies at the Loughborough University, and Professor of Popular Culture at the Erasmus University Rotterdam. Her work covers the articulation of popular culture and politics, for which she uses a wide range of standard and creative quantitative and qualitative methodologies. Professor Liesbet Van Zoonen is the corresponding author and can be contacted at: e.a.van-zoonen@lboro.ac.uk

Dr Georgina Turner is a Research Associate in the Department of Social Sciences at the Loughborough University. Her interests are media representations and discourses (and their production and consumption), identity in its personal, social and collective senses and the use of multiple and innovative methodologies. She also works as a journalist.