National Identity Infrastructures: Lessons from the United Kingdom

Aaron Martin

National Identity Infrastructures: Lessons from the United Kingdom

Aaron K. Martin

Information Systems and Innovation Group,
London School of Economics and Political Sciences, London, United Kingdom
a.k.martin@lse.ac.uk

Abstract Despite growing interest in the technologies of biometrics such as fingerprinting, facial recognition and iris scanning, there are too few in-depth case studies exploring their deployment on a national scale. This paper offers a qualitative analysis of biometric technologies by examining the National Identity Scheme – a recently abandoned United Kingdom government-sponsored program for a national identity card infrastructure. Leveraging organizing visions theory, it focuses in particular on government discourses about implementing a national infrastructure for biometrics. The discussion reflects on how the vision for implementing biometrics in the Scheme unravelled and tries to explain the course of these discourses in the political context of the UK.

Keywords: biometrics, case study research, e-government, failure, identification technology, organizing visions, surveillance

1 Introduction

Governments around the world are establishing new identity policies to apply new technologies to their civil registration and citizen identity systems [32]. Long-established forms of paper-based documentation such as identity cards, visas and passports are being upgraded with machine-readable zones, computer chips and radio frequency identification (RFID). These new 'smart' artefacts are promoted as being more reliable and secure than traditional paper documents. The latest trend is to include 'biometrics' in these documents in order to further secure identity infrastructures.

Biometrics are physiological or behavioural measurements, generally performed by computers, to identify someone or verify an identity. Examples of biometrics include facial recognition, fingerprinting, hand geometry, vein pattering, iris patterning, DNA profiling, signature recognition, keystroke dynamics recognition, gait recognition and speech or voice recognition, among other emerging and prospective techniques. Unlike conventional methods of secure authentication that rely on what you know (such as passwords, personal identification numbers (PINs) or cryptographic keys) or what

you possess (e.g., identity tokens or access cards), biometrics depend on facets of the human body – specifically what you are or what you do [21]. They are assumed to be a stronger means of identification because they cannot be forgotten or misplaced.

Following the terrorist attacks of September 2001, the Labour Government in the UK proposed a new identity policy that would take the form of a biometric-based identity card. What was originally uncontested later became politically controversial, taking four years to pass into law as the *Identity Cards Act 2006*. It then took a number of years to make progress in deploying the National Identity Scheme ("the Scheme") because of the unprecedented size and complexity of the proposals, including a centralized National Identity Register (the database on which the population's identity data would be held) and the recording of extensive amounts of personal information from individuals, including iris, fingerprint and facial biometrics. The government's plan for real-time, online biometric identification against a centralized, government-managed database was also a major innovation. In part because of the slow deployment of the Scheme, following a national election, the new Coalition Government repealed the law in December 2010, thereby cancelling the programme.

It is therefore important to study the discourses around a complex technology policy like identity policy, particularly when technologies like biometrics are introduced. A government-sponsored scheme for biometrics may bring with it a political dimension, often because of its compulsory nature, which is also an interesting source of data. This case study focuses on both the public and political discourses in the UK, as both were rich sources of data.

Motivated by theories on the role of discourse in organizing visions for new IT innovation, this paper seeks answers to the following question: To what extent were government spokespeople able to organize efforts and mobilize actors to innovate a national infrastructure for biometrics in the UK?

The remainder of the paper is structured as follows. First, I review the extant information systems literature on biometrics, exposing a dearth of in-depth case studies on the deployment of these technologies. Then I summarize the analytical framework, based on Swanson and Ramiller's organizing visions theory. Afterwards, I present the critical analysis of government discourses on the planned implementation of biometrics in the Scheme. The discussion offers an explanation for the course of the visions for biometrics in the case and the conclusion reflects on the paper's limitations and suggests areas for future research.

2 Critical Literature Review

While the technical literature on biometrics focuses on the details of trials and tests of various biometric techniques, the information systems literature is largely captivated by modelling user acceptance and surveying public perceptions of the technologies, with some exceptions (see, for example, [4] and [22]). Many consider the acceptance of biometric systems by user groups an important requirement for success. It is believed that without user acceptance, perfectly functioning systems are doomed to fail.

These studies focus on what Chau, Stephens and Jamieson [1] call the "people" side of biometrics. Some of this literature is inspired by the technology acceptance model (see, for example, [1], [11], [16-17]). Much of it lacks a theoretical grounding (e.g., [2], [5], [8-10], [20], [23]). Virtually all of this work is survey-based and hypothetical in nature. Respondents are asked to opine about biometrics without an understanding of the context of use or substantial engagement with the technologies in question.

One of the principal aims of these analyses of biometrics acceptance is to understand user resistance in order to overcome it, often through "better" marketing and information campaigns to "educate" uninformed consumers about the benefits of biometrics [1]. In many of these studies resistance to biometrics is viewed as a problem or as somehow irrational – the result of misunderstandings about the technology which ought to be corrected.

One grapples to make sense of the sometimes-contradictory findings of these studies. While some conclude that most users are ready to accept and use biometrics [24], others note on-going reluctance and potential resistance [20]. Some try to confront the unclear and contradictory nature of public opinion regarding these issues [10], [20], noting that understanding context and how exactly biometrics will be used by organizations is important. However, the literature lacks comprehensive studies on the real-world implementation of biometrics.

There is a good explanation for this: biometric systems are often spoken about, but rarely seen. This is partly to do with their novelty as well as the difficult political and technological environments in which they are pursued. While politicians speak with excitement about the possibilities of biometrics in achieving varying policy objectives, and deployment teams try to build the perfect environments for their solutions, few systems actually see the light of day in large-scale, real-world implementations. Biometrics are complex technologies that require vast technological, organizational and operational resources to operate seamlessly. As a result, there are insufficient cases of biometrics being used 'in the wild' and therefore the research investigations that typically study such systems once they are up and running have failed to materialize in substantial numbers. When biometrics are actually implemented for civilian purposes, typically in immigration applications, there is a void of objective information about their effectiveness and impacts. Border systems are often opaque and are not subjected to accountability measures applied to other government systems with which citizens interact. Similarly, to date many large-scale deployments of modern biometrics have been in non-democratic countries (e.g., UAE, Malaysia) where access to data is more challenging.

How then can we study such technologies? One way is to focus on the discourses around the proposals themselves, rather than waiting for the systems to appear. This case study therefore examines the organizational discourses that motivated the implementation of biometrics in the UK.

3 Theoretical Framework

The main theoretical construct that motivates this study is the 'organizing vision' in innovation projects [26-27], which provides a useful concept to help to explain the discursive emergence and development of IT innovation such as the government's pursuit of multiple biometrics in a national identity card programme.

Swanson and Ramiller aim to understand better the institutional processes that facilitate the adoption and use of new technology. In contrast to the traditional view that the early decision to adopt a given innovation happens as the result of local, rational organizational processes, which are subsequently institutionalized with the increased update of the technology, they argue that a better way of explaining innovation is as a collective process of creating and propagating an organizing vision that helps to coordinate decisions and actions related to the technology's materialization and diffusion. The organization vision can, thus, be understood as a sense-making device [30].

Organizations are frequently confronted with novel technologies that they perceive as demanding their attention: "New technology often arrives on the marketplace in an immature state, puzzling as to its benefits, future prospects, and long-term form" [27, p. 459]. Defined as "a focal community idea for the application of information technology in organizations" [27, p. 460], an organizing vision is thus intended to reduce, in broad strokes, the uncertainty that accompanies these new technologies. The organizing vision provides a conceptual framework that permits simplified understandings about novel and, as yet unsettled, technologies.

Swanson and Ramiller identify three main functions of an organizing vision:

- **Interpretation**: When a new technology arrives on the scene its meaning and implications are not well understood by organizational actors. It is in this space that organizing visions are generated to give some interpretive coherence to the innovation. They provide a focus for the innovation's interpretation [28, p. 556].
- **Legitimation**: These visions also give organizations reasons and justifications for pursing an innovation. They provide an answer to the question, 'why do it?' This legitimation process is facilitated through the reputations and authority of those promulgating the vision. To adapt an example from Swanson and Ramiller's paper to fit the case at hand, this process might be initiated as follows: "Why aren't we doing [biometrics] yet?" the [Home Secretary] might ask his or her [civil servant], having just read about it (and all the good things that come to leading [countries] doing it) for the first time in Business Week [27, p. 461].
- **Mobilization**: The organizing vision is a "creative force" that sparks and energizes market interest and activity to support the realization of the innovation. "Would be adopters look to the market for needed resources, including hardware,

software, and skills, following clues and guidelines embedded in the organizing vision" [27, p. 461].

Organizing visions are produced and sustained discursively, by a community with a common interest, which may agree or disagree about the content of the vision [27, p. 462]. The potential for disagreement means that there is an on-going contest of interpretations over the meaning of the technology. For Swanson and Ramiller, the depiction of the vision as an appropriate response to a certain business problematic will determine its currency and perceived relevance. Furthermore, the vision's perceived distinctiveness, intelligibility, informativeness and plausibility will also affect its compellingness and eventual success (or failure) [27, p. 469]. Importantly, there must be some new or emerging technology accompanying the vision that can be exploited by, but which also constrains, the vision. Often buzzwords (such as 'customer relationship management' [7] or 'enterprise resource planning' [29], or as in this present case, 'biometrics') play an important discursive role in signalling and strengthening the vision. However, there are risks to the overuse and overextension of such terms.

The organizing vision concept provides us with a core analytical tool to study imaginative discourse in innovation. Its emphasis on the early stages of discursive development, when understandings and outcomes about new technology are most uncertain, is especially apposite to the current case.

4 Research Methods

The analysis presented in this paper is the result of a multi-year case study of identity policy in the UK, focussing on the government discourses on biometrics. It is based on an exhaustive review of relevant government communications around the Scheme. The final corpus included every known public government document relating to the National Identity Scheme, published between July 2002 and December 2008. In total, there were 129 documents in this corpus, including:

- Legislative, parliamentary, research, and corporate publications
- Speeches and PowerPoint presentations by civil servants and ministers
- Interviews and interactive web chats
- Monthly newsletters (which were published by the Identity and Passport Service)
- Leaked government documents (which were made available to No2ID, the anti-ID card campaign group, and subsequently published on-line)
- Publicly-available responses to Freedom of Information requests

The analysis of documents is well established in social research [25]. To cope with the "attractive nuisance" of these qualitative data [19], the corpus was indexed in its entirety in the ATLAS.ti software for analysis, and then coded in accordance with principles and techniques from critical discourse analysis [6].

5 Analysis

This analysis encompasses official discourses on how the Home Office, the UK government ministry responsible for the Scheme, and the Identity and Passport Service, the department responsible for its deployment, would establish, run and manage a nationwide network of equipment for recording and reading biometrics. These discourses concern the organizations' knowledge, expectations and experiences of the design, development and installation of a new technology. These concerns are rife with future expectations about an implementation that, in the end, never happened.

5.1 Implementing Infrastructures

In practice, doing biometrics involves two major steps: the initial enrolment of biometrics from a person and the subsequent comparison of his or her biometrics against the previously enrolled data, during either an identification or verification mode.

From the beginning of proposals for the Scheme, the government paid considerable attention to how it might enrol the nation's biometrics. For example, noting the significant "learning curve" associated with implementing biometrics [12, p. 64], it sought opinions on this issue during the very first consultation exercise.

> The Government would like to hear the views of potential partners on how a nation-wide network of easily accessible biometric recording devices could be established and operated, how people who are not mobile or who live in sparsely populated areas could be served and what other value added services potential partners might offer. [12, p.110]

Such discourses explained the importance of providing biometric enrolment facilities in locations across the UK, and where that proved impractical the use of mobile recording devices.

> As well as local centres there will also be mobile centres for sparsely populated areas. [13, p.4]

However, much less attention was paid to how these enrolled biometrics would then be used in practice, particularly in ways that benefited the citizen whose data were being used. That is, the government's priority seemed to be figuring ways of collecting and storing everyone's biometrics in the first instance, and not how they would be subsequently used. Indeed, as a focus group interviewee from one of the early government's consultation exercises complained:

> For [biometrics] to be beneficial all these places would have to have finger scanning and eye scanning facilities. Otherwise it's pointless. [3, p.55]

One could argue that the government was especially focused on enrolment-related aspects because it is a necessary first step in the practice of biometrics and that other concerns would be addressed later on. Indeed, the government admitted in the begin-

ning that, in the initial stages of the Scheme, the use of biometrics would likely be limited, with the focus being on checking that people were not enrolling more than once.

> The use of any of the above types of biometric information (or a combination of these) would probably be limited in the early stages of an entitlement card scheme to ensuring that a person could not establish multiple, false identities. [12, p.105]

A further argument is that it was up to the organizations that would eventually use the Scheme to decide when and how they would make use of people's biometrics. That is, that it was the government's job only to provide the basic infrastructure for an identity scheme and that the eventual use of biometrics by public and private sector organizations should be demand-led and not dictated by the government.

However, the government's marketing activities for biometrics in the Scheme never extended beyond enrolment issues, with various attempts at forging relationships with organizations capable of enrolling large volumes of biometrics, without a clear explanation of how these would be used afterward. This further fuelled speculation amongst critics that the Scheme was one massive government data collection exercise, with little eventual benefit to the citizen. These suspicions were partly responsible for the Scheme's demise.

Another aspect of implementing an identity infrastructure based on biometrics has to do with the human resources required for such an undertaking, including both specialist training for facilitating and overseeing the enrolment process but also identifying and acquiring the expertise necessary for dealing with system errors and other anomalies as they emerge during biometric checking [cf. 4].

A major concern in government discourses was whether the public sector had suitable human resources to conduct large-scale biometric enrolment. At first, the need for trained specialists was downplayed by the Home Office.

> The Government envisages a much simpler scanning system than that used by the police or the Immigration Service, which would probably involve just the scanning of four fingers. The prints would not be scanned to a legal standard of proof of identity. *The staff taking the fingerprints therefore would not need to be as highly trained as those working for police forces of the Immigration Service and there would be no need for trained fingerprint officers to interpret the results of any potential matches detected by the computer*. [12, pp. 115-116, emphasis added]

Government discourses would shift in later documents, with revised claims that while expertise was needed, there were sufficient human resources already in the civil service on which to found an expert base. For example in the *Strategic Action Plan* the government stated:

> We will put in place the skills and expertise to support large-scale use of biometric matching. Biometric technology identifies small percentages of what are known as 'false matches' or 'false non-matches'. These need expert human assessment to ensure that matches are be-

> ing made correctly. For this, *we will build on resources which currently exist within government*. [14, p. 15, emphasis added]

Soon thereafter the discourses about biometrics training and expertise began to shift again, with the emphasis being placed on the need for 'support services'. As was admitted in the *Strategic Supplier Framework Prospectus*:

> With the use of probabilistic biometric matching technologies, there may also be associated biometric support services within this package (i.e. those services requiring expert human intervention). [15, p. 34]

The question, of course, was where this expertise would come from. While the government claimed that the UK Borders Agency was developing the relevant human resources through its programmes for collecting asylum seekers' biometrics and issuing biometric visas to foreigners, the size of these programs was dwarfed by the potential scale of a national identity programme. Concurrently, the government began articulating the need for "biometric enrolment services" for the Scheme, to be developed and provided by the market.

> The capacity to handle these enrolments – in terms of high street estates, personnel and technology – does not exist today. The Biometric Enrolment Service would need to deploy a nationwide capacity capable of handling five million+ enrolments a year, in a way that is convenient for customers, efficient and of high integrity. [15, p. 39]

Yet again, in these discourses the focus was on the human resources needed for the initial enrolment of biometrics for second-generation biometric passports (with fingerprint data) and identity cards, and not the human resources required for biometrics in various identification and authentication contexts. As previously noted, had the plans for biometrics matured and a significant number of people's biometrics been enrolled in the Scheme, this likely would have enhanced consideration of how biometrics would be used – including consideration of the attendant human resource implications. However, the Scheme was scrapped prior to the completion of contracting processes and these issues were never fully explored.

6 Discussion

The 'organizing vision' concept provides a means to understand how organizations seeking to develop and implement new technologies deal with their inherent uncertainties and ambiguities. By unifying and co-ordinating discourses and activities, organizing visions help to reduce doubts or unknowns about the future adoption and use of technology. With a single vision and a single goal, it becomes easier to implement new technologies, all the more so if potential defects and imperfections are discursively diminished. These discourses draw on a pool of conceptual resources that exist beyond the organization, and which are shared by a larger community that is also

interested in the technological innovation. When an organization brings together these cognitive and discursive resources in a cohesive manner, the organizing vision is said to be more stable, and thus sustainable. However, problems may arise – "where the innovation entails novel technology, this task can appear especially speculative and problematic" [27, p. 459]. In such cases, sustaining an unproblematic vision may prove difficult.

Organizing visions function to mobilize actors for the purposes of materializing an innovation. There were at three main groups of actors that the government aimed to mobilize in the case: the companies engaged to help the Home Office build the National Identity Scheme – including systems procurement and the outsourcing of biometric enrolment; a wide range of other public sector departments (which were expected to adopt the technologies and contribute to their diffusion); and the public, who were supposed to be the eventual end users of the system.

We will never know for certain whether the vision for biometrics would have successfully mobilized industry to develop and implement the biometric systems and services required for the Scheme had the Labour Party won the 2010 general election. By 2008, several firms had been engaged through the *Strategic Supplier Framework*, and certain contracts had even been agreed, but the programme for biometric identity cards was ended well before large-scale procurement and system design were completed. Before, during and after the election, we witnessed the demise of the Scheme, not because there were not any commercial actors willing to work with the Home Office, or because the technology failed to live up to expectations, but rather due to the course of political change. In brief, mobilization efforts were cut short by politics and in the process the debates about the technology's readiness, reliability and practicability were never entirely resolved.

As of 2010, none of the government departments that were expected to take up the biometric systems being developed for the Scheme had committed to using them (with the possible exception of the UK Border Agency, which was already collecting biometrics from foreigners). Champions of the Scheme had failed to mobilize these important organizational actors. But as before, this was arguably a matter of timing. The Home Office had cautioned that uptake by government departments would only begin once its identity infrastructure was in place. The election disrupted the original time frames for this project.

Finally, the third set of actors to be mobilized in the Scheme was the public. Suffice it to say, this was an enormous and diverse group of people, whose bodies were intended to be read, recorded and repeatedly validated by biometric devices. Their mobilization was especially critical to the Scheme's success but the government's programme for identity cards and new (fingerprint) biometric passports was terminated before the public were to begin enrolling their biometrics *en masse*. The systems required for mass enrolment were never implemented. Critics such as No2ID had argued that it was at the point of mass enrolment that public resistance would mount, but this is a hypothesis that remains untested. What is known is that by the time the Scheme was finally abandoned, only 14,670 Britons had volunteered for an identity card. A significant fraction of these – nearly 3,000 airside workers from select airports – received their identity cards for free. In addition, an unknown number of the enrollees were civil servants who were privately encouraged to apply for an identity card before the election [18].

What can we learn from this episode? The project for a national identity infrastructure based on biometrics was unsuccessful for a number of reasons:

- **Organizational complexity**: The Scheme was a Labour Party policy, which the Home Office and Identity and Passport Service were responsible for implementing. The presence of multiple actors from such varied organizations (including both politicians and civil servants in this case), who are responsible for articulating and co-ordinating a coherent vision for new technology is something that the organizing visions theory (as articulated in Swanson and Ramiller's original article) does not easily accommodate. Historically, organizing visions theory has focused on the institutionalization of an innovation within a single organization, rather than looking at visions spanning multiple organizations, and which voyage into 'society at large'.
- **Scale**: The Scheme was a huge undertaking, encompassing not just the Home Office, but also eventually the entirety of government and certain private sector organizations (such as banks). Moreover, a successful Scheme would require some degree of participation from national public and certain classes of foreign citizens. It is highly debatable whether such top-down visioning and innovating is possible on this scale, especially considering the range of organizations, people and bodies involved.
- **Politics**: A vision for the implementation of an enterprise resource planning system in a business organization, for example, may encounter resistance, which may even be political in nature; however it is unlikely to be tightly bound to notions of citizenship, freedom and identity. The government's proposals for biometric identity cards, by contrast, elicited considerable political distrust, fears of government tracking 'innocent' citizens and worries about privacy intrusions, as was represented in the political opposition's discourses as well as media reports on the Scheme [31]. There is therefore a qualitative difference between visions for a corporate accounting system, for instance, and a nationwide, government-sponsored identity system. The former is a solution to a problem. The latter is a political choice about how society should look and be organized, where the search for a solution may precede the event of a problem. Where the 'need' for such a large communal effort seems the stuff of choice and not necessity, political opposition is always difficult to surmount. Not surprisingly then, the proposals became highly politicized over time as the urgency which supposedly underpinned them grew more and more elusive. These politics affected the content of the vision for biometrics, with the government reworking its messages to focus on themes of 'empowerment' and 'inclusion' as the Scheme's fate grew more and more uncertain.

7 Conclusion

The widespread introduction of biometrics has proven to be controversial in the UK, but this is not an inevitable outcome. Some argue that a national infrastructure for

biometrics would represent a sea change in identification practices. Others argue that in a modern world the collection of this information is inevitable and no longer sinister. These debates are ongoing.

This chapter focused its analysis on publicly available discourses, as one must surely do with such a topical matter of public security provision where classification and industrial secrecy loom large. I would have liked to get inside the organizations responsible for delivering the Scheme in order to gain access to those individuals responsible for overseeing its creation, design and implementation. These include civil servants in the Home Office and Identity and Passport Service, whom I believe would have provided an interesting source of data. However, this was not possible for various reasons, the most obvious of which was the sensitivity of the project and institutional concerns about protecting what was said to be 'commercially confidential' and 'security sensitive' information regarding the programme.

Finally, this research project was a single case study. Future research should aim for comparative analyses. Two other national programmes for biometrics (namely, Mexico and India, both of which aim to enrol multiple biometrics including irises) have been recently launched and would make interesting comparative cases.

References

1. Chau, A., Stephens, G., Jamieson, R.: Biometrics Acceptance – Perceptions of Use of Biometrics. In: Proceedings of the 15th Australasian Conference on Information Systems. Hobart, Tasmania, Australia, pp. 1–6 (2004)
2. Clarke, N.L., Furnell, S.M, Rodwell, P.M., Reynolds, P.L.: Acceptance of Subscriber Authentication Methods For Mobile Telephony Devices. Computers & Security, 21(3), 220-228 (2002)
3. Cragg Ross Dawson: Identity cards – People with special issues: Response to the proposed customer experience report (2004)
4. Davis, C.J., Hufnagel, E.M.: Through the Eyes of Experts: A Socio-Cognitive Perspective on the Automation of Fingerprint Work. Management Information Systems Quarterly, 31, 681-704 (2007)
5. Deane, F., Barrelle, K., Henderson, R., Mahar, D.: Perceived acceptability of biometric security systems. Computers and Security, 14(3), 225-231 (1995)
6. Fairclough, N.: Critical Discourse Analysis: The Critical Study of Language. Longman, New York (2010)
7. Firth, D.: The Organizing Vision for Customer Relationship Management. In: Proceedings of the 7th Americas Conference on Information Systems. Boston, Massachusetts, USA (2001)
8. Furnell, S.M., Dowland, P.S., Illingworth, H.M., Reynolds, P.L.: Authentication and Supervision: A Survey of User Attitudes. Computers & Security, 19(6), 529-539 (2000)
9. Furnell, S., Evangelatos, K.: Public awareness and perceptions of biometrics. Computer Fraud & Security, 2007(1), 8–13 (2007)
10. Heckle, R.R., Patrick, A.S., Ozok, A.: Perception and acceptance of fingerprint biometric technology. In: Proceedings of the 3rd Symposium on Usable Privacy and Security, pp. 153–154. ACM, Pittsburgh, Pennsylvania, USA (2007)

11. Ho, G., Stephens, G., Jamieson, R.: Biometric Authentication Adoption Issues. In: Proceedings of the 14th Australasian Conference on Information Systems. Perth, Western Australia (2003)
12. Home Office: Entitlement Cards and Identity Fraud: A Consultation Paper. Stationery Office, London (2002)
13. Home Office: Identity Cards Briefing (2005)
14. Identity & Passport Service: Strategic Action Plan for the National Identity Scheme: Safeguarding Your Identity. Home Office, London (2006)
15. Identity & Passport Service: National Identity Scheme Strategic Supplier Framework Prospectus. Home Office, London (2007)
16. James, T., Pirim, T., Boswell, K., Reithel, B., Barkhi, R.: Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model. Journal of Organizational and End User Computing, 18(3), 1-24 (2006)
17. Jones, L.A., Antón, A.I., Earp, J.B.: Towards Understanding User Perceptions of Authentication Technologies. In: Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, pp. 91-98. ACM, Alexandria, Virginia, USA (2007)
18. Lettice, J.: ID card astroturf - No2ID beats the truth out of IPS. The Register (2010)
19. Miles, M.B.: Qualitative Data as an Attractive Nuisance: The Problem of Analysis. Administrative Science Quarterly, 24(4), 590-601 (1979)
20. Moody, J.: Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use. In: Issues in Informing Science and Information Technology. Rockhampton, Australia, pp. 753-761 (2004)
21. O'Gorman, L.: Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, 91(12), pp. 2021-2040 (2003)
22. Otjacques, B., Hitzelberger, P., Feltz, F.: Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. Journal of Management Information Systems, 23(4), 29-52 (2007)
23. Perakslis, C., Wolk, R.: Social Acceptance of RFID as a Biometric Security Method. IEEE Technology and Society Magazine, 25, 34-42 (2006)
24. Ponemon Institute: Global Study on the Public's Perceptions about Identity Management. Unisys Corporation, USA (2006)
25. Prior, L.: Using Documents in Social Research. Sage, London (2003)
26. Swanson, E.B.: Talking the IS Innovation Walk. In: Wynn, E.H., Whitley, E.A., Myers, M.D., DeGross, J.I. (eds.) Global and Organisational Discourse about Information Technology, pp. 15-32. Kluwer, Boston (2003)
27. Swanson, E.B., Ramiller, N.: The Organizing Vision in Information Systems Innovation. Organization Science, 8(5), 458-474 (1997)
28. Swanson, E.B., Ramiller, N.C.: Innovating Mindfully with Information Technology. MIS Quarterly, 28(4), 553-583 (2004)
29. Wang, P.: 2009. Popular Concepts beyond Organizations: Exploring New Dimensions of Information Technology Innovations. Journal of the Association for Information Systems, 10(1), 1-30 (2009)
30. Weick, K.E.: Sensemaking in Organizations. Sage, Thousand Oaks, CA (1995)
31. Whitley, E.A.: Perceptions of Government Technology, Surveillance and Privacy: the UK Identity Cards Scheme. In: Neyland, D., Goold, B. (eds.) New Directions in Privacy and Surveillance. Willan, Cullompton, UK, pp. 133-156 (2009)
32. Whitley, E.A., Hosein, G.: Global Identity Policies and Technology: Do We Understand the Question? Global Policy, 1(2), 209-215 (2010)