Characteristic trade-offs in designing large-scale biometric-based identity management systems

Siraj A. Shaikh\textsuperscript{a,}\textsuperscript{*}, Joseph R. Rabaiotti\textsuperscript{b}

\textsuperscript{a} Department of Computing and the Digital Environment, Faculty of Engineering and Computing, Coventry University, Priory Street, Coventry CV1 5FB, UK
\textsuperscript{b} Centre for Forensic Computing and Security, Department of Informatics and Sensors, Cranfield University, Shrivenham, Swindon SN6 8LA, UK

Article info

Article history:
Received 17 August 2009
Received in revised form 20 December 2009
Accepted 31 December 2009

Keywords:
Biometrics
Identity management
Accuracy
Scalability
Privacy
UK
Passport
Identity cards

Abstract

Biometric-based identity management systems are deemed to be the new solution to address the challenges of global security and citizenship. While such systems do prove effective, the nature of biometric technology, the costs involved, and increasing threats to theft and loss of data bring with it a variety of other considerations that cannot be ignored. We approach such systems from the perspective of large-scale high-volume public deployments. We find that various characteristics of such deployments present a trade-off, where emphasis on one undermines the other. Such characteristic trade-off spaces are described and explored in this paper. The ultimate contribution lies in the understanding of such trade-off spaces for the purposes of optimal design of such systems. We use our approach to analyse the recently launched Identity Card scheme in the United Kingdom.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

Biometric-based identity management is increasingly being used by governments and national agencies, amongst others, for identity verification and law enforcement. While many laud the use of biometrics as an efficient and scalable option, many others challenge the shortcomings in terms of loss of privacy, and the potential for fraud and abuse. Large scale implementation of such systems brings with a variety of new challenges. Given the critical context it becomes imperative that such systems are thoroughly assessed for fitness for purpose. In this paper we concern ourselves with large scale biometric-based identity management systems: high-volume, high-usage implementations, primarily deployed at a national (or cross-national) level for the purposes of immigration, identity and passport, driver and vehicle licensing, crime, transport, health, social security or other public administration.

At the core of any decision to deploy large scale biometric-based infrastructure for identity management lie three critical factors, namely accuracy, scalability and privacy. We define these three notions for the purposes of this paper. Accuracy refers to the precision level of verification of identity. This is more than just biometric template matching as it involves a desired level of confidence to be established in the identity of the subject being verified. So, for example, immigration officials, in addition to fingerprint matching, often look to verify the relevant travel history of a foreign traveller coming into the country. They check the traveller’s stated record against the number of previous entries into the country and the duration of each visit. A matching record serves to assure the officials of the identity of the individual with respect to the travel documents carried. Scalability refers to the features of the technology that makes it suitable for deployment at busy high-volume locations. This includes a broad set of features, from a variety of perspectives, that are all relevant to a large scale implementation. From an operational perspective, this includes processing performance, cost of deployment including infrastructure (such as storage, processing and communication), operation (in terms of required technical staff amongst others) and maintenance, and the level of manual assistance required at the point of operation. From users’ perspective, acceptability (due to social and cultural issues) and the ease of biometric sample capture are important. Such acceptability is a key consideration for systems designed for high volume use, which is what we are concerned with. This is partly because it feeds into public satisfaction, and also as it serves to be the perceived benefit of deploying automated systems providing fast and seamless identity verification for the masses.
**Privacy** refers to the preservation of the ability of individuals to control their personal (biometric and other) data. Such control applies to appropriate use and storage of personal data. Of interest here are the potential threats to the individual's control and consent over personal data. Such threats result from data loss or leakage, behaviour profiling, surveillance or any other inappropriate use of personally identifiable information.

Different stakeholders involved in such deployments will place greater emphasis on some criteria over others. This is understandable given the different nature of their concerns. **Biometric technologists** strive to reduce false positives and false negatives with a view to making the technology more accurate and efficient, ultimately with an interest in its success.

Governments, on the other hand, have a different set of priorities as recently many governments have come under much criticism for choosing to spend public funds on stricter identity management regimes. In United Kingdom, for example, the public opinion has turned against the recently launched Identity Card scheme. A public survey conducted in July 2009 reveals that 79% of the British population is of the opinion that 5bn—the cost of the scheme—could be better spent in other areas of the economy (Public Servant, 2009). Support within the British government is also waning as easing the public spending crisis becomes more of a priority for an increasing number of elected officials (Morris and Brown, 2009; Young, 2009). In the face of this, national agencies are keen to promote the scalability and economic feasibility aspects of such schemes. Cost is not the only concern here. For such schemes to operate at high-traffic environments, such as airports, convenience and usability features are also key. This is demonstrated by the recent trials of facial recognition technology at Manchester and London Gatwick airports, where the British Government, and the UK Border Agency in particular, have emphasised on reduction in queues and the ease in processing of people (McKeegan, 2009; Clifford, 2009).

Privacy rights campaigners have a different agenda altogether. Their main concern is the protection of civil liberty and privacy, upholding the record and storage of as little information as possible about individuals. In the UK, for example, public campaign groups such as NO2ID1 and DEFY-ID,2 have scrutinised the Identity Card scheme and expressed serious doubts over the risks to basic freedoms and privacy of individuals subject to the scheme (Grossman, 2009). But herein lies the conundrum: measures to preserve privacy are available but only at the cost of accuracy and scalability. Accuracy often comes at a cost of sacrificing scalability and more importantly privacy. Large scalable deployments, on the other hand, favour technologies that are less accurate and often do, as the evidence suggests, threaten privacy.

The question is how do we decide what technology to deploy? How do we evaluate the different technologies available for their fitness for purpose? Moreover, what system design principles underpin the various objectives involved here? Undoubtedly, it is difficult to propose a single solution to such a multi-objective design problem. There is a need, however, to explore the trade-off space offered here. This will help in comprehending the design and implementation issues, and addressing the challenges involved. The aim of this paper is to delve into the characteristics trade-offs for biometric-based identity management deployments. We characterise the relationship between the three important characteristics of such systems identified above: a simple **trade-off triangle** is presented for the purposes of illustration. The underlying idea is simply that each of the characteristics is related to another representing a trade-off. This relationship between each pair offers a trade-off scale, which is used to determine the influence on the system as a result of the design decisions made. Such decisions are to do with a range of lower technological level choices to system level design to higher policy level considerations, including

- the choice of biometric technology, and multimodal operation,
- system level features, such as capture of biometric data,
- data handling, storage and communication involved, relevant to database design and any distributed processing involved, and
- legislative, security and privacy concerns.

We then use our approach to analyse the recently launched Identity Card scheme in the United Kingdom. Each of the three trade-offs are examined in relevant detail. The particular example used here serves as an ideal problem to analyse for large scale implementation.

### 1.1. Rest of this paper

The rest of this paper is organised as follows. Section 2 discusses some related work. Section 3 presents the central idea of this paper. We present the idea as a simple illustration, which is then analysed further in the sections that follow. A pairwise collection of three trade-off scales: accuracy–privacy, accuracy–scalability and scalability–privacy are each analysed in Sections 3.1–3.3, respectively.

Section 4 then delves into the biometric-based identity management systems in the UK. A particular attention is paid to the recently launched Identity Card scheme by the UK Government. We analyse the scheme with respect to our proposed characteristic trade-off space. Section 5 finally concludes the paper.

### 2. Related work

Jain et al. (2004) define a biometric as any human physiological and/or behavioural characteristic that satisfies certain requirements (it must be universal, distinctive, permanent and collectable). However, they set out three further requirements for a practical biometric system (performance, acceptability and resistance circumvention) and, whilst this work is not concerned with circumvention resistance, the Jain category “performance” encompasses the categories of accuracy and scalability used in this paper. They do not propose any trade-off with respect to the characteristics of the technology.

Schouten and Jacobs (2009) present an evaluation of the Netherlands’ proposed implementation of a biometric passport, largely focusing on technical aspects of specific biometric technologies (such as face and fingerprint recognition) but also making reference to international agreements and standards (such as ICAO and the EU’s “Extended Access Control”) and discussing the privacy issue in terms of traditional security concepts such as confidentiality.

Grijpink (2006) presents an assessment model for the use of biometrics which conceptualises new technology, biometrics in this case, as a **spoiler** if applied to a problem from an administrative perspective rather than an **informant** if applied from a judicial perspective. The model is presented to avoid creating obstacles when new technology is applied to solving existing issues.

---

1. [http://www.no2id.net/](http://www.no2id.net/)
problems. It is not clear whether such a model could be usefully applied to a wider set of biometric-based deployments, apart from the biometric passport example that Grijpink (2006) has discussed briefly.

Some other related work focuses on privacy issues. Grijpink (2008) discusses the various mechanisms used to avoid storing biometric data either on tokens or centrally on databases, and instead storing some irreversible representation of it which can then be compared every time an individual is to be authenticated: a fresh sample is obtained and processed to a similar representation and then compared with the stored value. Shaikh and Dimitriadis (2008) adopt a more critical view towards privacy implications for such systems. They argue that biometric systems pose a critical trade-off with privacy from a variety of legal, technical, social and psychological perspectives. There is no attempt made, however, to specifically relate the specific issues raised due to scalability of such systems and what privacy issues are implicated as a result.

A general overview of the literature highlights a particular absence of any attempt to relate the various features of biometric systems, and any attempt to discuss the experiences derived from the implementation and operation of large-scale public deployments.

3. Characteristic trade-offs

We propose a trade-off triangle, the underlying idea of which is simply that emphasis on any one of the relevant characteristics, namely, verification accuracy, scalability or privacy, results in the undermining of the other two. The triangle shown in Fig. 1 helps to illustrate this simple relationship.

The three respective edges in Fig. 1 represent the trade-off space between each of the two characteristics of large-scale biometric-based deployments: if accuracy is the most important design requirement for a biometric deployment, there must be compromises in scalability and privacy. Likewise, a system designed for maximum privacy will have less-than-optimal accuracy and scalability, and optimally scalable systems are likely to score less highly on accuracy and privacy.

The trade-off between each pair of requirements is examined in detail in the rest of this section. Each section highlights the relevant design challenges for such systems and the resulting influence on the corresponding choices to be made. An understanding of this trade-off space presents an indicator of desirable features when designing such deployments; such an understanding is largely the important aim of this paper.

3.1. Accuracy vs. privacy

Verification accuracy receives a lot of attention given the drive for perfection in biometric technology. Moreover, the technology is increasingly being deployed for critical applications such as immigration control and national identity management. Given that this is being done in the context of national security, and often as a response to terrorism, the emphasis on greater levels of precision for identity verification is obvious. Such deployments as a result are increasingly being designed to improve upon verification accuracy, which in turn stands to erode privacy.

3.1.1. How much data?

The more personal data available, both to store and process during verification, means more likelihood for achieving better accuracy. This comes with a heightened risk to privacy, however, as more information is at risk of leakage and manipulation. This is possibly the simplest relationship to express, and may be modelled by considering the number of personal data items used in the system. As the number of data items increases, we can expect accuracy to increase, but collecting and storing a larger number of data items constitutes more of a privacy problem, both in itself and because more data being stored and transmitted increases the chance that some of it might leak. An example of this is the use of multimodal biometrics: using a single biometric trait is increasingly being seen as a limitation due to:

- noisy sensed data,
- non-universality (Daon, 2002),
- poor distinctiveness (inherent to the particular biometric trait),
- variation (due to sensor interoperabilities), and
- potential spoofing attacks.

3.1.2. Multimodal biometrics

A system based on multiple biometric traits provides means to overcome most of the above weaknesses and increase confidence in verification decisions (Indovina et al., 2003). The more biometric modalities used therefore means the more accurate the identification. This also has a higher impact on the individual should the private data be compromised, however. In essence, improving accuracy requires more data to be held, whereas privacy demands otherwise.

3.2. Accuracy vs. scalability

Verification accuracy is undoubtedly critical but so is scalability for such systems. The trade-off between these two is possibly the most critical, and introduced primarily due to system technological reasons. Apart from the nature of the biometrics, the requirements for data communication, processing and storage influence this space. A factor critical to scalable deployments is cost. This includes the cost of infrastructure, operation and maintenance.

For large-scale deployments, such costs could pose as a serious obstacle. According to an early estimate of the General Accounting Office (GAO) (investigative arm of America’s Congress, and America’s National Academy of Science (NAS)), the biometric systems at US border-crossing points, part of the US-Visit program, cost US$ 1.4 bn–2.9 bn initially, and US$ 700 m–1.5 bn annually thereafter (Economist, 2003). Considering that such costs usually come out of national security budgets, it becomes imperative to justify them against other security measures. In hard economic times, this is even more difficult.
3.2.1. Which biometric?

Collecting sample biometric data is a highly repeated operation in biometric-based deployments. The relative ease of sample collection is therefore very important at busy high-population locations. Some biometric traits allow for a more easier sample collection than others. Voice and facial recognition, for example, allow easier collection than fingerprint or iris recognition, which necessitate touch or very close proximity. Evidence suggests that biometrics typically associated with easier sample collection perform at a much lower level of verification accuracy than those that do not: for example Jain et al. (2004) find that voice, facial and gait recognition perform at a relative low level of accuracy than fingerprint or iris recognition which perform at a high level. Jain et al. (2004) define such performance in terms of

- accuracy,
- speed,
- resources required to achieve an acceptable level of accuracy and speed, and
- operational and environmental factors affecting accuracy and speed.

Such evidence demonstrates a critical trade-off, which in this case is due to the very nature of the biometric technology. Contact (or very close proximity) may serve to be a key differentiator here for the technology. Note that sample collection is an issue both at enrolment and verification stages (Coventry, 2004), but undoubtedly much more critical for the latter given the high volume.

3.2.2. Multimodal biometrics

Other mechanisms employed to improve upon accuracy demonstrate a similar relationship. The use of multimodal biometrics only serves to raise the scalability challenges in terms of

- a higher cost of biometric sensors, as more of different types are needed,
- higher computational resources to process more data from multiple sources, and
- additional delay in sample collection due to both multiple biometrics and the likely manual intervention required as a result (particularly a concern at busy deployments such as airports).

All of which undermine the scalability of biometric-based deployments.

3.2.3. Communication, processing and storage

Verification accuracy stands to benefit immensely both from the availability of more personal data and multimodal biometrics, as discussed in Sections 3.1.1 and 3.1.2. A variety of other system data may also be used from a design perspective (such as identifiers for collating data from different databases). Altogether this comes with an increase in costs of communications, processing and storage of data; a detailed breakdown of which includes cost associated with

- more data collection and storage per individual, essentially leading to bigger databases,
- higher processing and memory capacity for terminals,
- higher bandwidth communication channels, linking terminals to servers and databases, and
- additional delay in processing, possibly introduced to processing and verifying additional information for each individual.

3.2.4. False matching

The potential for false matching makes biometric technology inherently vulnerable to identity fraud. Such fraud is a more serious concern for large public deployments where physical characteristics of two different people passing as one are much more likely (Schneier, 2004). False matching is a serious security concern and, as such, any false match rate greater than infinitesimal is unlikely to be tolerated. Hence the need for using multimodal biometrics and verification of other personal details to confirm identity, all of which come at an extra cost (Most, 2004), and hence undermine scalability as highlighted in Section 3.2.2. The higher the volume of individuals, the higher the probability that someone, somewhere at some stage will get through the net when s/he should not. A failure, albeit one in a million, as such stands to raise serious questions, not to mention tarnish the reputation of such systems.

Note that the above trade-off serves to not only put scalability of such systems at odds against accuracy, but also against privacy. The identity fraud that could potentially result is likely to cause greater inconvenience to the victim of such a crime. Any measures to enforce privacy effectively on such scale are not viable given the likely legal (Woodward, 1997), technological (Most, 2004) and social costs (Venkatraman and Delpachitra, 2008).

3.3. Scalability vs. privacy

Loss of any identifiable information means potential risk of identity theft. Loss of biometric data is more serious since the loss is permanent. Fingerprints and facial images are very personal and permanent to humans, the misuse or abuse of which is disastrous for the privacy of individuals. Large-scale public deployments, which inevitably leads to increased processing and communication of such data, not to mention storage in some form or representation, is potentially a cause for concern for individual privacy. Such deployments throw up a variety of privacy issues that we highlight in the rest of this section.

3.3.1. Loss of privacy due to automation

One major reason for automating as much of the biometric identification process as possible is to provide increased scalability (albeit at a greater initial cost). A properly designed automatic system should be quicker and more convenient than an equivalent human-operated one, and it should also be more cost-effective in the long term. However, such systems make it possible to process and store considerably larger amounts of data, bringing with it enhanced risks of leakage and manipulation. For instance, on any given day, customs and immigration officials at a busy international airport will examine thousands of passports from hundreds of different countries. It is relatively easy for a human to determine that the picture on the passport matches the bearer, and for an experienced customs official to determine if the passport itself is suspicious, for example, a likely fake. In order for an automated system to achieve the same goal, it has to communicate and process personal data, possibly over public communication channels and shared terminals.

3.3.2. Data security

For large scale deployments the risks to personal data are very high as handling, processing and storage on such a scale brings with it

- accidental data loss (Wilson, 2007),
- a potential target for hackers and terrorists (Johnson, 2004),
- linkability of personal data (Anderson et al., 2009), which allows for profiling and for
3.3.3. Design aspects

A biometric-based identity management system is clearly less private than a non-biometric-based system, since more (personal and particularly biometric) data is stored. The non-biometric option offers much less scalability due to the time taken to establish an individual's identity (through manual means); the risk of loss of personal data, however, is avoided.

For biometric-based systems, the design with respect to authentication of individuals is of interest. If the individuals' data are stored on a database and is accessed every time there is a need to authenticate, then it probably does away the need for a token. Such an option offers greater scalability in terms of costs. But the storage, processing and communication of such data (or any representation of it) throws up severe risks for compromise (in terms of data loss, theft and breach). Recent instances of such breach in the UK (Stringer, 2009) serve as harsh reminders. Such mishaps could certainly be avoided if biometric (and other personal) data is not stored on any database.

The other option is store biometric data (or some representation of it) on tokens. This has the advantage from a privacy perspective as personal details are not stored (or processed or communicated with) on any central database; any risks that arise from such a scenario are devoided therefore. This serves to raise the costs for tokens (be it smart cards, passports or any other), along with costs involved in handling, printing/processing and replacement. It is not too difficult to see the severe trade-off that the (authentication) design aspects of such systems raise, with respect to privacy and scalability.

3.3.4. Legislative and regulatory requirements

A variety of legal and regulatory standards, including ICAO passport regulations and data protection regulations (such as EU Data Protection Directive 95/46/EC Parliament, 1995), for the use of biometrics and especially with regards to the design of identity management systems (such as ID cards and passports) make such deployments very costly. The enforcement of such legal and technical mechanisms, necessary to protect public data, makes it very difficult (in terms of costs and design) to develop systems that meet often contradictory requirements.

The EU Data Protection Directive, for example, emphasises on transparency that ensures that individuals give their explicit consent before their personal data is being processed. Moreover, individuals have the right to access all their personal data, and also modify or control incomplete or inaccurate data. The directive also emphasises proportionality to ensure that the personal data processed is not excessive or inadequate for the purposes of its usage.

The controls needed to satisfy such requirements manifest in various forms to ensure that

- individuals are provided with a choice, where possible, to opt out (or opt in as the case may be) of the recording of any personal data,
- individuals are made conscious of the capture of their personal data, and where feasible, is done so with their consent,
- individuals are comprehended about the precise state of their captured data, and its future use,
- personal data are confined for the precise purposes of what it was captured for, and
- the context of the use of such data is very carefully designed for and provably demonstratable if needed arises.

Such controls are immensely costly to implement, and even costlier to maintain and operate for the lifetime of such systems.

A concern with the EU Directive (and other similar mechanisms) is the exceptions and opt-outs due to concerns for national security. State authorities would often resort to use national security concerns to access personal data. This asks for provision to be built in for access, which in turn is not cheap to implement. For public-level large scale implementations, a more serious concern is the lack of trust that develops as the authorities use such tactics; even a single case could seriously undermine public support for such systems.

4. Biometric-based identity management in the UK

4.1. Overview

The United Kingdom has not had an identity card since the Second World War, but proposals to reintroduce it have been made sporadically since then. The concept of an identity card containing biometric information is somewhat more recent, and initial feasibility studies for the current scheme undoubtedly began before 2000. A 2001 bulletin from the UK’s Parliamentary Office of Science and Technology (2001) cites two case studies, one of which refers to biometric identification systems which were, at the time, being introduced on an experimental basis at US airports to allow frequent travellers to transit immigration more quickly. Rather than going before a human immigration official, the travellers would use an automated terminal to confirm that their hand geometry matched a record stored on a card which they carried (it is not stated whether any central databases were also used by this system). The human immigration official would only be called in if the match failed. This system (INSPASS) was eventually dismantled, but a similar system (NEXUS) currently operates between the United States and Canada to allow citizens of either country who frequently cross the border to expedite the immigration process. The NEXUS system uses both fingerprints and iris images as biometric identifiers.4

In 2003 a more thorough feasibility study was carried out by the National Physical Laboratory on behalf of the UK Passport Service, the Driver and Vehicle Licensing Agency and the Home Office (Mansfield and Rejman-Greene, 2003). The study concluded that the use of either four fingerprints or two iris scans would be sufficient to uniquely identify any individual from the country’s population of the UK. However, they go on to state that “...the practicalities of deploying either iris or fingerprint recognition in such a scheme are far from straightforward” and that “current biometric systems are not designed for civil application of the scale envisaged in the UK entitlement scheme.” The study also found that, on the basis of the systems they evaluated, enrolment was by far the costliest aspect (see Mansfield and Rejman-Greene, 2003, p. 29). It could thus be said that the biometric technologies extant at the time of the Mansfield study provided sufficient accuracy but not scalability (of course, considerable progress has been made since then, so this is not necessarily applicable to modern biometric systems).

Meanwhile, when the International Civil Aviation Organisation (ICAO) was devising a standard for e-passports which incorporated biometric data, they decided to use face recognition. Compared to

fingerprints or iris recognition, face recognition has the significant advantage that, since passport applicants are already used to providing photographs and the necessary biometric data may be generated from these, enrolment is a vastly easier process, though it does become necessary to impose more stringent conditions on photograph quality.

The issue of how the biometric data is transmitted and stored is also significant for privacy. In the UK, the Home Office has introduced biometric passports (Home Office: Identity and Passport Service, 2009), which use a storage microchip which can transmit the biometric data to a special reader using RFID. This provides for a quick and smooth operation as it only requires the passport to be placed in proximity to the reader, and hence is very scalable. The wireless transmission of information, however, implies that it may also be intercepted, or that it may be “read” from a greater distance. RFID devices are only designed to work over small distances, but successful attacks have already been mounted over greater distances using special equipment (Juels et al., 2005). The use of RFID thus can be seen to increase scalability at the expense of privacy.

The UK Border Agency makes use of biometrics in its Iris Recognition Immigration System (IRIS) (UK Border Agency, 2009). It claims that this can reduce the time taken to clear immigration to about 20 s, a significant increase in scalability (although users must first enrol in the scheme, which can take up to 10 min). The biometric data are not stored on the passport, but in a central database. The use of a central database avoids the privacy issues associated with transmitting the data from the passport, but introduces new ones concerning the security of the database. Sections 1.12 and 1.13 of the IRIS Scheme Definition Document (UK Government, 2009) state that the “iris images will be stored in encrypted form in a secure archive database, to which access will be strictly controlled” and that “additional information, such as a person’s name, date of birth, nationality, gender, passport details ..., will also be recorded as part of the enrolment application process”. Whilst the IRIS scheme is still voluntary and restricted to a few airports, the volume of data handled by the central database is likely to increase, and so will the potential for leakage.

4.2. UK national identity cards

The UK National Identity Card scheme is defined by the Identity Cards Act 2006 (UK Government, 2006). The scheme uses smartcards containing three biometric identifiers (fingerprints, facial photograph and signature, though the Act allows for others—see Schedule 1 section 2d). Other information may also be stored on the card, but the majority of the information stored is in a back-end database known as the National Identity Register. Schedule 1 of the Identity Cards Act specifies the different categories of data which may be stored in the register, but does not specify exactly which of these are also stored on the identity card. This is probably to allow maximum flexibility in the actual deployment. Schedule 1 of the Identity Card Act gives nine broad categories of data stored, which are as follows (for the full list of information from Schedule 1 see Appendix A):

1. **Personal information** (including full name, addresses, date and place of birth, and gender).
2. **Identifying information** (the biometric data).
3. **Residential status** (Nationality, citizenship status, entitlement to reside in the UK, etc.).
4. **Personal reference numbers** (potentially encompassing any and all ID cards, passports, immigration documents, driving licences, and other official documentation).
5. **Record history** (details of any changes to the data in the register, and date of death).
6. **Registration and ID card history** (dates and particulars of applications for ID cards and for changes to data held in the register).
7. **Validation information** (essentially recording how the details supplied by the individual were verified at each stage of the application or change process).
8. **Security information** (for storing identification number, password, security questions, etc., to allow individuals to apply online to view their entry in the register or get modifications made).
9. **Records of provision of information** (to record when the register is accessed by third parties).

The “identifying information” section specifies that the Identity Register may store a photograph of the subject’s head and shoulders (showing facial features), a signature, a set of fingerprints, and “other biometric information”. This is clearly intended to be open-ended and allow for an unlimited number of future biometric identifiers to be added. The Identity Cards Act does not specify which items are stored on the identity card itself, probably because the card had not been designed yet. The final design for the identity card to be issued to British citizens has only recently been released, and the government plans to make them available on a voluntary basis in the Greater Manchester area at the end of 2009, with the aim then being to expand nationwide by 2011 (BBC, 2009). The Immigration and Passport Service web site (Identity and Passport Service, 2009a) shows a card which stores various information in human and machine-readable format, and also contain a “smart” chip which stores additional information. Some information also appears to be stored in multiple formats, whereas other data items only appear once.

There are two machine-readable data sources on the card; in addition to the smartcard chip there is also an optically readable “swipe zone” similar to those found on machine-readable passports. This consists of three rows of 30 characters, and examination of the specimen photographs seems to indicate that the first row stores an identifier (“IDGBR”) and what is presumably the 10-digit card number, the second row storing (among other things) the holder’s date of birth and the card’s expiry date in YYYMDDD format, and the final row storing the holder’s surname and given name(s).

Table 1 shows which items of personal data are stored on the card and in what form (based on the information provided by the UK Identity and Passport Service in (Identity and Passport Service, 2009c). In this table, “MRZ” stands for “Machine-Readable Zone”.

It should be noted that the specimen card image given in the BBC News articles was of the version intended for British citizens; the versions intended for EU/EEA citizens and other foreign nationals residing temporarily in the UK have distinctive colouration and other minor differences. The data printed on the card is stored in a manner which is intended to resist fraudulent reproduction, and there are a number of security features which may be checked by a human examining the card (Identity and Passport Service, 2009b). It is not clear whether any of these features may be checked by an automated reader, since specifications of such readers have not been made available.
Although all the data stored on the card are in a sense personal, not all of them are equally easy to extract from the card. Before considering the specific data items that are stored on the UK ID card, it is possible to define categories based on ease of access:

- Data that can simply be read from the card in passing.
- Data that requires extended access to the card (e.g. the machine-readable zone, which is human-readable with a bit of effort).
- Data that cannot be obtained without extended access and special equipment (data stored in the smartcard chip).

In practice, many data items are duplicated and appear in more than one category, thus even though the card holder’s date of birth is stored on the smartcard chip, it is not necessary to interrogate the chip to obtain these data because it is also printed on the card (see Table 1 for other such duplications).

Schouten and Jacobs (2009) make two significant points in the context of fingerprint storage on biometric passports. First, they state that fingerprints are usually stored as compressed images because of the lack of a standard template. If the fingerprints in the UK ID card are stored in this format, they are at greater risk of being extracted in a useful fashion. Second, they refer to the Extended Access Control protocol—a scheme based on Diffie-Hellman key exchange which allows the storage chip and reader to authenticate each other before data are transferred—and state that this is an EU requirement for protecting fingerprint data (German government, 2008). It would be interesting to know if the smartcard chip in the UK ID card uses a similar authentication mechanism, or indeed any authentication mechanism—the only information on this subject which the Immigration and Passport Service provides is the statement that “The card’s high integrity design incorporates security features compliant with European and International Civil Aviation Organisation (ICAO) standards. In addition, the data on the chip will be protected, such that the data cannot be changed, modified or cloned” (Identity and Passport Service, 2009a).

### Table 1 Data stored on the current British identity card.

<table>
<thead>
<tr>
<th>Data item</th>
<th>Visible on card</th>
<th>On MRZ</th>
<th>On smartcard chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Number</td>
<td>Yes</td>
<td>Yes</td>
<td>Unknown</td>
</tr>
<tr>
<td>Surname</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Given name</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Gender</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Place of birth and nationality</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Signature</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Facial image</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Date of issue and expiry date</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

4.2.2. Accuracy vs. scalability

As far back as the National Physical Laboratory study in 2003 (Mansfield and Rejman-Greene, 2003) it has been recognized that enrolment costs would represent a significant proportion of the total cost of implementing a biometric identification scheme. As per Section 3.2.1, the choice of biometric is critical here. A photograph probably represents the simplest form of biometric as far as enrolment is concerned, since similar photographs are used for passports and facilities to have suitable pictures taken are readily available. This is not true of fingerprints, which must be collected using special equipment.

Furthermore, a picture may also be verified by an untrained human, which is not true of a fingerprint match; for this reason it is necessary that fingerprints be provided in person and that additional steps to confirm identity are taken at the enrolment stage (see Mansfield and Rejman-Greene, 2003, p. 9). Of course, it is fairly obvious that the more biometric factors are used—see Section 3.2.2—the more complicated the processes of enrolment and verification will have to be. This has an impact on scalability in terms of usability and cost.

4.2.3. Privacy vs. scalability

The fact that at least two of the biometric identifiers on the ID card may be checked by a human in the absence of automated equipment means that the card is more scalable (since scalability is affected by the expense of installing special equipment and coping when it breaks down) but also less private, because the details which are intelligible to a human are also easily copiable. A lost or stolen identity card would give a criminal the name, date of birth and signature of the cardholder without too much effort. How much additional information is obtainable will depend on

---

7 On the subject of fingerprints, it is interesting that only two fingers are used in the scheme given that the study undertaken by the National Physical Laboratory in 2003 recommended using at least four. However, the NPL study did not include facial biometrics, and did in fact say that, “Face recognition biometrics ... might be used in the checking process, thereby possibly reducing the number of fingers required.” (see Mansfield and Rejman-Greene, 2003, p. 10).
how well the smartcard chip is protected, since the machine-readable zone does not appear to contain anything useful that is not already printed in more intelligible form.

The use of the back-end database is also interesting. It could be argued that the use of a central database reduces the amount of work that needs to be done by the local verification system and thereby reduces the complexity (and therefore cost) of the cards and readers. If more sensitive details are stored in the back-end database rather than on the card, there is less need for costly security measures to protect the data on the card. The design trade-offs from Section 3.3.3 clearly apply here.

Furthermore, the heightened risks to centralised storage at this scale (see Sections 3.3.2 and 3.3.1) cannot be discounted. Any gains in scalability are also losses in privacy; for instance, it is proposed that the back-end Identity Register database should record how many times it has been accessed and for what purpose. If it is necessary to access the database every time someone’s identity is to be confirmed, it will be impossible to use an identity card without leaving a permanent record in the database. This permanent record could easily be used (or abused) for surveillance and tracking purposes (as acknowledged in Section 3.3.2).

From the details available on Identity Register, it is not clear how privacy and civil liberties are going to be protected using the UK or EU legislative measures available for this purpose. Such measures potentially stand to drive up costs, as discussed in Section 3.3.4, as the system becomes operational and conflicts arise.

5. Conclusion

This paper has explored characteristic trade-offs for large scale deployments of biometric-based identity management systems. A trade-off triangle, presented in Section 3, illustrates our simple relationship between the accuracy, scalability and privacy aspects of such deployments. The national Identity Card scheme in the UK is analysed as a case study in Section 4.

Our characterisation of biometric technologies ultimately aims to serve as a basis for systemic design and implementation of biometric-based identity management, particularly for deployment in the public domain. A systematic approach to implementing such infrastructures allows the stakeholders involved, identified in Section 1, to agree on desired criteria and devise optimal deployments. Such an effort also serves to help better public understanding of the trade-offs involved here as the relationship between the three criteria becomes more transparent.

The three characteristics discussed here, namely the verification accuracy, scalability and privacy, are all major concerns for the various stakeholders in such systems. More importantly, the common public, arguably the biggest stakeholder, is ideally interested in systems that live up to all three: accuracy is critical as it, if designed to serve the purpose, protects national security. Scalability is important as it helps reduce the costs of such systems and hence be less of a tax burden. Privacy is undoubtedly of interest to us all as it concerns the well-being of our personal information and inevitably us. The trade-off space then becomes ever so crucial. It allows us to determine the qualities of our biometric-based identity management systems carefully. For most societies, privacy is of utmost importance. Accuracy and scalability aspects, however, cannot be undermined in more security-conscious societies and less-developed countries, respectively. Our work serves to inform the policy from either of these perspectives.

For future work, we propose to derive a classification of biometric technologies based on the three characteristic trade-offs analysed in this paper. This should serve to facilitate a language, cutting across the technological and social spheres, which the stakeholders involved can use to reason and analyse biometric-based identity management systems.

Acknowledgements

We are grateful to the anonymous reviewers for their valuable feedback which has helped to improve the ideas presented in this paper.

Appendix A. The Identity Cards Act 2006

The following is quoted verbatim from Schedule 1 of the Act.

A.1. Information that may be recorded in register

Personal information

1. The following may be recorded in an individual’s entry in the Register—
   (a) his full name;
   (b) other names by which he is or has been known;
   (c) his date of birth;
   (d) his place of birth;
   (e) his gender;
   (f) the address of his principal place of residence in the United Kingdom;
   (g) the address of every other place in the United Kingdom or elsewhere where he has a place of residence.

Identifying information

2. The following may be recorded in an individual’s entry in the Register—
   (a) a photograph of his head and shoulders (showing the features of the face);
   (b) his signature;
   (c) his fingerprints;
   (d) other biometric information about him.

Residential status

3. The following may be recorded in an individual’s entry in the Register—
   (a) his nationality;
   (b) his entitlement to remain in the United Kingdom;
   (c) where that entitlement derives from a grant of leave to enter or remain in the United Kingdom, the terms and conditions of that leave.

Personal reference numbers etc.

4. (1) The following may be recorded in an individual’s entry in the Register—
   (a) his National Identity Registration Number;
   (b) the number of any ID card issued to him;
   (c) any national insurance number allocated to him;
   (d) the number of any immigration document relating to him;
   (e) the number of any United Kingdom passport (within the meaning of the Immigration Act 1971 (c. 77)) that has been issued to him;
   (f) the number of any passport issued to him by or on
5. The following may be recorded in an individual’s entry in the Register—

(a) information falling within the preceding paragraphs that has previously been recorded about him in the Register;
(b) particulars of changes affecting that information and of changes made to his entry in the Register;
(c) his date of death.

6. The following may be recorded in an individual’s entry in the Register—

(a) the date of every application for registration made by him;
(b) the date of every application by him for a modification of the contents of his entry;
(c) the date of every application by him confirming the contents of his entry (with or without changes);
(d) the reason for any omission from the information recorded in his entry;
(e) particulars (in addition to its number) of every ID card issued to him;
(f) whether each such card is in force and, if not, why not;
(g) particulars of every person who has countersigned an application by him for an ID card or a designated document, so far as those particulars were included on the application;
(h) particulars of every notification given by him for the purposes of regulations under section 11(1) (lost, stolen and damaged ID cards etc.);
(i) particulars of every requirement by the Secretary of State for the individual to surrender an ID card issued to him.

7. The following may be recorded in the entry in the Register for an individual—

(a) the information provided in connection with every application by him to be entered in the Register, for a modification of the contents of his entry or for the issue of an ID card;
(b) the information provided in connection with every application by him confirming his entry in the Register (with or without changes);
(c) particulars of the steps taken, in connection with an application mentioned in paragraph (a) or (b) or otherwise, for identifying the applicant or for verifying the information provided in connection with the application;
(d) particulars of any other steps taken or information obtained (otherwise than in connection with an application mentioned in paragraph (a) or (b)) for ensuring that there is a complete, up-to-date and accurate entry about that individual in the Register;
(e) particulars of every notification given by that individual for the purposes of section 10.

8. The following may be recorded in the entry in the Register for an individual—

(a) a personal identification number to be used for facilitating the making of applications for information recorded in his entry, and for facilitating the provision of the information;
(b) a password or other code to be used for that purpose or particulars of a method of generating such a password or code;
(c) questions and answers to be used for identifying a person seeking to make such an application or to apply for or to make a modification of that entry.

9. The following may be recorded in the entry in the Register for an individual—

(a) particulars of every occasion on which information contained in the individual’s entry has been provided to a person;
(b) particulars of every person to whom such information has been provided on such an occasion;
(c) other particulars, in relation to each such occasion, of the provision of the information.

References