Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2008 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2008

Biometrics and the United Kingdom National Identity Register: Exploring the privacy dilemmas of proportionality and secondary use of biometric information

Aaron K. Martin
The London School of Economics and Political Science, a.k.martin@lse.ac.uk

18F. Biometrics and the United Kingdom National Identity Register: Exploring the privacy dilemmas of proportionality and secondary use of biometric information

Aaron K. Martin
The London School of Economics and Political Science
a.k.martin@lse.ac.uk

Abstract

Despite the obvious importance of privacy concerns in the information age, “privacy” remains a messy concept in the academic literature. Scholars are thus attempting to clarify and systematize the privacy concept. They have proposed two important dimensions of privacy concerns: 1) *proportionality,* or the adequate, relevant and non-excessive collection of personal data, and 2) *secondary usage,* or the prohibition of subsequent, unspecified uses of personal information.

This paper takes measure of the proportionality and potential secondary uses of biometric data in the proposed United Kingdom (UK) National Identity Register (NIR). It argues that the UK Identity Cards Act 2006 fails to guard against violations of the principles of proportionality and secondary usage of biometric data.

After reviewing the modern literature on informational privacy protection, I analyze biometrics and their privacy implications. I then discuss these implications in the context of the UK government’s NIR plans. The analysis yields insights into how biometrics on the proposed NIR interplay with purpose specifications, architectural concerns, knowledge asymmetries and public anxieties. I also explore potential secondary uses of the types of biometric data that could be stored in the NIR. Last, a brief note is offered about the possible means of regulating against privacy infringements.

Keywords

Privacy, proportionality, secondary usage, biometrics, UK National Identity Register, Identity Cards Act 2006

1. Introduction

Around the world, organizations of varying size and purpose are moving towards increased identification standards. National governments are amongst these organizations, as they grow ever more concerned with collecting and sharing information about the identities of citizens and foreign visitors.

On 30 March 2006, the UK Parliament passed legislation enabling a National Identity Scheme (NIS), with a key component being a national database of personal information called the National Identity Register (NIR). The purposes of the scheme as put forth in the UK Identity Cards Act 2006 include the facilitation of information about individuals in the UK to those reasonably requiring proof. Importantly, such facilitation must only occur when in the “public interest”. In the Act, “public interest” encompasses: 1) national security; 2) the prevention or detection of crime; 3) immigration control; 4) the enforcement of prohibitions on unauthorized working or employment; and 5) securing the efficient and effective provision of public services.

In this paper I argue that, despite the UK government's seemingly good intentions, the current proposals do little to address concerns about proportionality and abuse of recorded information. I also argue that, in practice, the broad notion of "public interest" might increase the likelihood of privacy infringements by providing a catchall justification for data collection and use. The UK government's plans are further compromised by its poor performance record in terms of safeguarding citizens' personal data, especially in light of recent security breaches at Her Majesty's Customs and Revenue (HMRC), the UK tax agency. The collection, storage, processing and subsequent use of biometric information on the UK NIR introduces unresolved privacy dilemmas, particularly with respect to the principles of proportionality and aspects of secondary usage of data. These issues must be considered, deliberated and protected against prior to the widespread collection and storage of biometric information.

2. Conceptualizing privacy

There is a rich, diverse, and multidisciplinary body of literature on privacy. This literature includes contributions from law, regulation, sociology, psychology, and, increasingly, from management and technology. Yet, numerous authors have noted the difficulty of conceptualizing and defining privacy; its slipperiness and vagueness often results in misunderstandings about alleged violations. Recognizing this, Daniel Solove has formulated what he calls a taxonomy of privacy in order to "shift focus away from the vague term of 'privacy' and toward specific activities that pose privacy problems" (2006, pp. 481-482). Although Solove's analysis is placed in the US context, I suggest that his framework can be usefully extended to privacy concerns in the context of the UK NIS. While the current analysis is specifically concerned with the principle of proportionality and problems of secondary usage of data, I briefly outline Solove's taxonomy so as to better understand its implications in the larger privacy arena.

Echoing Davies (1998, p. 93), Solove aptly notes that modern day privacy problems are generally architectural in nature. These architectural risks "involve less the overt insult or reputation harm to a person and more the creation of risk that a person might be harmed in the future" (2006, p. 487). Two types of architectural risks frequently emerge: 1) the enhancement of risk of future harm and 2) imbalances of social and institutional power. In Solove's taxonomy, there are four main categories of harmful activities under which different subcategories fall. These include: 1) information collection, 2) information processing, 3) information dissemination and 4) invasion (p. 488). I discuss each in turn.

2.1 Information Collection

Solove identifies two information collection activities: *surveillance* and *interrogation*. The former becomes problematic when done in a certain manner, say continuously or surreptitiously (2006, p. 493). *Surveillance* is a tool of social control because it tends to result in self-censorship and inhibition. Performed covertly, it is worrisome because it may have so-called chilling effects, whereby speech or conduct is suppressed or restricted out of fear of penalties. However, eliminating secrecy from surveillance does not necessarily make it desirable or acceptable. As Jeremy Bentham's Panopticon demonstrates, even an awareness of the possibility of surveillance can inhibit behavior (Solove, 2006, p. 495).

Moreover, Solove observes that, while the law often addresses surveillance, it does so quite narrowly and under what he coins the “secrecy paradigm”:

> Under the secrecy paradigm, privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information. In many areas of law, this narrow view of privacy has limited the recognition of privacy violations (2006, p. 497).

Surveillance is thus potentially harmful in all settings, not just private ones, as public surveillance can cause uneasiness and distrust.

The second form of data collection, *interrogation*, involves pressuring individuals to disclose concealed information, often creating discomfort and distortion (pp. 500-501).

2.2 Information Processing

The information processing dimension of privacy involves the ways collected information is stored, manipulated and used. Solove’s taxonomy divides information processing concerns into the following subcategories: *aggregation*, *identification*, *insecurity*, *secondary use* and *exclusion* (2006, p. 505).

Data aggregation is the gathering together of bits of information that by themselves are not very telling. When combined, these data begin to form a more detailed profile of an individual. New information technologies have made data aggregation easier and cheaper, leading to novel architectural problems (p. 507).

Following Roger Clarke (1998), Solove defines *identification* as “the association of data with a particular human being” (2006, p. 510). It entails a link to a person in the flesh and attaches informational baggage to people (pp. 510-511). Moreover, identification creates architectural problems insofar as it increases government control over people (p. 513).

Insecurity is a problem caused by the mishandling and poor protection of personal information, often resulting in identity theft. Solove remarks that despite the law’s reluctance to find harm simply from the insecure storage of information, insecurity does indeed result in one being placed in a weakened state and made more vulnerable (p. 518).

Secondary use is “the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject’s consent” (p. 519). Proportionality and secondary usage are tightly intertwined concepts. Various privacy principles and laws acknowledge secondary usage as a serious problem by prohibiting it through what are known as *purpose specification principles* (pp. 519-520). For example, Article 6 of the EU ‘Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data’ (Directive 95/46/EC), specifies that member states shall ensure that all personal data are:

- “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed” (EU Directive, 1995).

Closely related to the problem of secondary usage is what Paul Schwartz calls the asymmetry of knowledge problem (1999, p. 1683). About this Solove notes:

> …even with privacy policies stating that information might be used in secondary ways, people often do not read or understand these policies. Nor can they appropriately make an informed decision about secondary uses **since they might have little idea about the range of potential uses** (2006, p. 520, emphasis added).

Solove notes two further problems with secondary use. The first is that it generates fear and uncertainty concerning future uses of collected data, thus instilling a sense of powerlessness and vulnerability among data subjects. In addition, secondary data usage can create architectural problems related to risk of future harm in that information may not fit well with new uses. Once these data are decontextualized, the potential for misunderstandings increases (p. 520).

Finally, *exclusion* is failing to provide data subjects with information and input about their records (p. 521). It too creates an architectural problem as it reduces organizational accountability to those data subjects with records on file.

2.3 Information Dissemination

This category of privacy harms encompasses revelations of personal data as well as threats to do so. Solove understands information dissemination as including such acts as *breach of confidentiality*, *disclosure*, *exposure*, *increased accessibility*, *blackmail*, *appropriation*, and *distortion*. I review each briefly.

Solove defines *breach of confidentiality* as revealing secrets about someone in a way that violates trust in the relationship (2006, p. 524). Related to this is the third party doctrine, by which information possessed or known by third parties is not subject to a reasonable expectation of privacy. This third party doctrine is based on the secrecy paradigm and especially relevant in the information age.

Disclosure occurs when "certain true information about a person is revealed to others" (p.529). When revealed publicly, such information may be used in unforeseeable ways, thus paralleling the problems of secondary usage. *Exposure* resembles disclosure in that both involve the release of true information. Yet, whereas disclosure entails the release of information with which others may judge the data subject's character, the information involved in exposure lacks such significance. According to Solove, "exposure creates injury because we have developed social practices to conceal aspects of life that we find animal-like or disgusting" (p. 534).

The privacy harm associated with increased accessibility is indirect in nature. It is an enhancement of risk of disclosure and the problems thereof. With *increased accessibility* comes the potential for using data in ways neither originally conceived of nor originally intended (p. 537). For Solove, *blackmail* is harmful because it permits the control of the data subject by means of threat and distortions in relational power (p. 540).

Appropriation is "the use of one's identity or personality for the purposes and goals of another" and takes on two dimensions; the first is related to dignity and the second to property rights. Solove recognizes that most contemporary claims of misappropriation are argued in terms of property rather than dignity, noting, "Loss of property seems to be more readily recognized by courts today than the more amorphous feelings of embarrassment or loss of dignity” (p. 544). Last, *distortion* involves inaccurately portraying a data subject and covers such phenomena as false light, defamation and record system inaccuracies (p. 546).

2.4 Invasion

The final category of privacy harms includes two types: *intrusion* and *decisional interference*. *Intrusions* are “invasions or incursions into one’s life” and include such things as spam and telemarketing (pp. 549-550), while *decisional interference* is government interference in decisions related to a data’s subject life (p. 554). Solove argues that decisional interference resembles secondary usage in that both can have chilling effects on a data subject’s relationship with her/his body. This point is especially relevant to an analysis of biometrics.

3. Basic biometric concepts

Having reviewed Solove’s taxonomy of privacy, here I present the basic concepts of biometrics before moving onto the particulars of the case.[1]

Biometrics consist of physiological or behavioral measurements. The former include facial geometry, fingerprinting, hand geometry, vein pattering, iris patterning and DNA profiling, among others. The latter involve such characteristics as signatures, keystroke dynamics, gait and speech or voice[2], and are occasionally referred to as behaviometrics (Nisenson, Yariv, El-Yaniv, & Meir, 2003, pp. 363-364). Unlike conventional methods of identification that rely on what you know (passwords, cryptographic keys) or what you possess (tokens, cards), biometrics depend on the human body itself: on what you are and what you do (Zviran & Erlich 2006).

It is generally agreed that, to qualify as a biometric, a bodily measurement must satisfy certain requirements. According to Jain, Ross and Prabhakar (2004), bodily features should be: 1) universal, 2) distinct, 3) relatively permanent and 4) collectable. Universality means that all participants in a scheme possess the characteristic. If this is not the case, then compulsory participation would prove difficult to enforce. Alternatively, multiple biometrics might be employed in the case of non-universality, as was originally proposed in the UK upon realization that not everyone in the UK may have readable fingerprints, for example. The distinctiveness requirement aims to prevent situations in which different people share the same characteristic. For example, using height (a common bodily measurement) as a biometric identifier would be very challenging in this respect. Permanence is important in that a rapidly changing identifier would result in live biometrics not matching their stored counterparts, thus undermining the system wholesale. The quantitative measurability of a biometric determines its collectability (Jain et al., 2004, p.4).

There are certain steps that must be taken before a biometric scheme can be said to be operational. These include the initial capture of biometric data across a population, the subsequent processing or conditioning of these data for storage purposes, feature extraction

[1] This section intentionally excludes a discussion of the various technical shortcomings associated with biometric systems as the effectiveness of the technologies involved is not under investigation in this paper. For a thorough review of the known limitations, errors and failures inherent to biometric systems, see O’Gorman (2003).

[2] Usually characterized as a behavioral biometric, voice does have an underlying physiological component (O'Gorman, 2003).

and template generation. Note that while actual raw biometric images may be saved for administrative reasons (Clarke, 2001), most often compressed, feature-extracted templates are stored and compared against live data captures.

3.1 Images versus templates

There is a general understanding that, for biometric systems, featured-extracted templates of biometric images that are stored in databases instead of the images themselves. For example, certain system implementations collect information about the fingerprint or measurements of the face rather than collecting a complete image of the finger or face. However, this is not universally true. For instance, forensic applications do store original images (Faundez-Zanuy, 2005, p. 14). Also, for systems of such grand scale and complexity as a national identification scheme, it may be necessary to record and file original images in the event that a decision is made to implement another vendor's proprietary technology (including algorithms, templates, scanners, middleware and databases). The current lack of biometric standards means that new templates would have to be reprocessed from original images. Presumably, re-recording an entire national population's biometrics in person would prove an administrative nightmare, hence the perceived need to store these original images.

3.2 Multimodal biometric systems

It is also widely believed that the use of multiple (multimodal) biometrics for recognition is more reliable than systems that rely on a single (unimodal) biometric trait (Jain & Ross, 2004; Lazarick, 2005). Supposedly, multiple, distinct pieces of biometric information may be combined to address certain problems that plague biometric systems, namely hacking (Faundez-Zanuy, 2004), spoofing (Matsumoto, Matsumoto, Yamada, & Hoshino, 2002) and the non-universality of particular biometric features in the population (Jain & Ross, 2004, pp. 37-38). For example, someone without hands, thus incapable of providing fingerprints, might present her/his irises to a biometric reader instead. Multimodal systems have even been described as a positive for privacy. Faundez-Zanuy argues that certain privacy concerns may be resolved by "using a multimodal biometric system, where the user can freely decide between several biometric identifiers, and reject the system that he considers may reveal private information" (2005, p. 15).

4. The case of the UK NIR

As mentioned, the proposed UK NIR is just one component of a larger scheme. According to the Strategic Action Plan published by the UK Home Office (2006, p. 7), the interior ministry responsible for the scheme, other principal elements include such documents as identity (ID) cards and passports, as well as such procedural elements as applications, identity checks and background checks. While the ID card and passport are the most highly publicized components of the scheme and are often the focus of heavy media coverage (Martin and Whitley 2007), it is the databases which comprise the NIR that are of primary concern in this analysis. According to the Act, over 50 types of personal information may be stored on the register for each individual.

In its original conception, the NIR was to be a single, massive database, created anew, in which all information would be stored together for each individual (Identity Cards Act, 2006). However, this changed in December 2006 when the department responsible for administering the scheme, the UK Identity and Passport Service, housed within the Home Office, released its Strategic Action Plan to set out a revised database schema for the register (UKIPS, 2006). At present, a set of different databases is envisioned on which biometric, biographical and administrative information are to be separated.[3] The stated reasons for this segregation include increased security and making use of “the strengths of existing systems” (UKIPS, 2006, p. 10). However, it is still unclear whether this separation of data is to occur logically or physically.

4.1 Biometrics and the NIR

Clarifications were also made in the Strategic Action Plan regarding the use of biometrics in the identity scheme. Four biometric features were explicitly mentioned in the original Act: fingerprints, facial photographs, iris patterns and signatures[4] (2006). In fact, the Act defined ‘biometric information’, as “data about [an individual’s] external characteristics, including, in particular, the features of an iris or of any other part of the eye”. However, the December 2006 Strategic Action Plan downplayed the role of irises, noting that:

> When you enrol into the Scheme, your fingerprint biometrics (all 10 fingerprints) will be recorded and stored in the National Identity Register. A subset of these will be held on your ID card or passport, in line with International Civil Aviation Organization standards. **The introduction of iris biometrics also remains an option** (UKIPS, 2006, p. 16, emphasis added).

Notably, the latest government report on the ID cards scheme, *The National Identity Scheme Delivery Plan 2008*, released in March, makes no mention of irises.

It appears the decision to drop or postpone the introduction of iris biometrics in the NIR results from concerns about costs (because iris scanning technology is significantly more expensive than, say, fingerprinting) and international obligations (because there is no international consensus on iris scanning), although some have speculated that the poor performance of current technology is to blame (Espiner, 2007). However, it should be noted that the minimal formal International Civil Aviation Organization requirement is a digital facial photograph. States are given the option to supplement this with fingerprint or iris images but by no means is this obligatory.

5. Privacy analysis of the NIR

Here I focus on what is known and unknown about the NIR at present in assessing it in terms of its proportionality and potential secondary usages.

5.1 Proportionality

5.1.1 Unclear purpose

As Zorkadis and Donos state, “respecting the principle of purpose implies an understanding of, first, a clear definition of the purpose for which the biometric data is collected and processed” (2004, p. 131). One may argue that the purpose(s) for which biometric data are to be collected for storage on the NIR are not clearly defined. The umbrella of “public interest” lacks the clear specification required by principles of proportionality. Moreover, the all-

[3] According to the Strategic Action Plan, the systems to be reused are biometric systems used for asylum seekers and biometric visas, the Department of Work and Pensions (DWP) Customer Information System (CIS) technology and existing Identity and Passport Service (IPS) systems (2006, p. 10-11).

[4] While signature analysis is considered a reliable behavioral biometric method, traditional, static signatures are not. It is still uncertain which of these is to be included in the NIR, although it is most likely the case that only static images of signatures will be stored. Jones, Antón, & Earp (2007) note that the distinction between traditional signatures and signature analysis as a biometric method is a point of confusion for many users.

encompassing reasons enumerated in the Act (2006), namely national security, crime prevention and detection, immigration control, restricting unauthorized work and improved provision of public services, are so broad as to be uninformative if not dangerous. For instance, in the contemporary political climate in which a growing number of deviant activities are deemed contrary to national security interests, one must consider potential scenarios in which biometric information might be abused by public authorities, say at political gatherings and public protests.

Controversy regarding government databases and proportionality is not without precedent. As publicized by the watchdog organization Genewatch (2006), the UK national DNA database (UK NDNAD) has witnessed its share of disproportionate uses. To quote the report at length:

> Research using the Database is supposed to be restricted to the purpose of detecting or reducing crime. However, this has been interpreted broadly by the Board to include research on predicting characteristics such as ethnicity from DNA. There is nothing to prevent future research without consent using either the Database or samples, potentially including controversial topics such as searching for 'genes for criminality'.

This loose interpretation of purpose in the UK NDNAD foreshadows a potentially wide array of misuses and abuses of biometric data stored on the NIR. Recently, there has even been speculation by former Home Secretary Charles Clarke about linking the UK NDNAD and NIR (Buchanan, 2007). Whether this is to happen is difficult to predict, but the prospect speaks to the gruesome potential for disproportionate use of the NIR.

5.1.2 Architectural problems

Certain things must also be noted about architectural problems of the NIR based on information available in the December 2006 Strategic Action Plan. At issue is the first type of architectural problem identified by Solove: the enhancement of risk of future harm. The centralization of a massive amount of biometric data, even if separated from bibliographical and administrative data as mentioned in the strategic action plan, lends itself to abuse by officials. Pooling together the biometric data of the entire UK population significantly increases the risk of a breach. The recent loss of data on all UK families by HMRC provides a cautionary tale.

5.1.3 Asymmetry of knowledge

Also of concern is the general lack of specificity by the government concerning the ways biometrics are to be collected, stored and processed by the various systems. For one, it remains unclear whether original images are to be recorded and filed somewhere for administrative purposes. Moreover, there has been no public discussion regarding the need for multimodal biometrics as well as whether and how they are to be fused (Jain & Ross 2004, pp. 38-40). For example, are scanned biometrics to be recorded locally on readers during the verification process? If so, then there might be additional privacy risks on local machines – as was recently discovered in photocopiers in which all copied and scanned images were stored on disk drives, unbeknownst to users (CNN, 2007). Unfortunately, very little information about such system components has been publicized, and thus asymmetries of knowledge persist. To make matters even more confusing, the government recently announced in its March 2008 Delivery Plan that it seeks to create a "market" for biometrics enrollment rather than handling biometrics enrollment itself. This focus on reducing costs introduces huge data protections concerns and engenders further knowledge asymmetries regarding the collection, storage and processing of biometric data.

Furthermore, the aforementioned likelihood of dropping iris information from the NIR jeopardizes the entire case for a multimodal system. However, the UK government remains silent on this point. If we take Faundez-Zanuy's point for granted, that multiple biometrics are a good thing for privacy because users may choose which biometric to employ, thus keeping secret the biometric of their choice, then the exclusion of irises may be understood as harming privacy (or at least perceptions thereof).

5.1.4 Fear and uncertainty

According to Solove, two further harms related to proportionality are fear and uncertainty. There exists good reason for fear and uncertainty amongst the UK public concerning potential harms caused by the storage and use of biometric information by authorities. In particular, the case of Shirley McKie does very little to quell these misgivings. McKie, a police officer in Scotland, faced a decade of legal troubles and financial hardship due to a botched crime scene fingerprint analysis. Her thumbprint was supposedly recovered at a murder scene despite her adamancy about having never been present at the crime scene. The handling of her case by fellow police officers and politicians did much harm to public perceptions of fingerprinting, especially with respect to the involvement of officials in the process (see HMIC (2000) for more information). The introduction of biometrics into a day-to-day nationwide identity scheme might encounter similar, if not worse problems.

5.2 Secondary usage of biometric data

While very little is known about the technical specifications of the biometric systems to be used in the NIR outside of the kinds of biometrics that might be employed, it is still possible to speculate about potential secondary uses of the biometric data intended for the register.

5.2.1 Known and possible uses of biometric data

In addition to forensic uses of information such as fingerprints, there are other known and possible uses of biometric data that deserve attention.

- High resolution photographs of the eye have been shown to indicate whether a patient suffers from diabetes, arteriosclerosis or hypertension, among other ailments (Faundez-Zanuy, 2005, p. 13). Depending on the use of templates in the NIR, or whether original images are saved in some system for administrative purposes, this sort of information may be obtainable by those with access to certain parts of the register, such as civil servants. If this information were accessed by insurance companies, then data subjects might face additional difficulties in insuring themselves.
- Bowyer, Hollingsworth and Flynn (2008) point to recent research with the objective of predicting ethnicity based on a person's iris image (Qiu, Sun, & Tan, 2006). Moreover, others have demonstrated the ability to predict gender by analyzing irises (Thomas, Chawla, Bowyer, & Flynn, 2007). They conclude that "these works point out a possible privacy issue arising with iris biometrics, in that information might be obtained about a person other than simply whether their identity claim is true or false" (Bowyer et al., 2008, pp. 27-28).
- Faundez-Zanuy cites studies which suggest that fingerprints and finger images might disclose such medical information as whether a person is affected by Downs syndrome, Turner syndrome, Klinefelter syndrome, intestinal obstruction, leukemia, breast cancer and Rubella syndrome. He also cites a study linking fingerprints and homosexuality (2005, pp. 14-15).[5]

[5] Even if the science behind these claims is not credible, the fact that it is being undertaken speaks to potential secondary usage of data issues.

- One possible secondary use of facial images is in compiling mug shots for witnesses of crimes. It is not certain whether such usages fall under the purposes of the scheme and register, namely crime prevention and detection. Arguably, there are serious ethical and privacy concerns at issue in this use of facial images.
- Last, access to large stores of signatures might prove handy to those engaged in credit card or check fraud. It is hoped that technical protections such as encryption would be used to protect signature data, but at present details are unclear.

5.3 Possible modes of regulation

The question of how to prevent the abovementioned privacy violations is a difficult one. With the UK NDNAD in mind, it seems that largely legal means of regulation are ineffective in practice, especially considering the presumed complexity of the systems involved in the NIR. One might also argue that it is possible to regulate privacy through the technology itself (Lessig, 1999); however, regulation by means of code alone might prove insufficient. According to Solove, "privacy problems… are caused not by technology alone, but primarily through activities of people, businesses, and the government. The way to address privacy problems is to regulate these activities" (2006, p. 560). With that in mind, it appears an appropriate course of action is through improved laws protecting biometric privacy, combined with certain technologies such as encryption or, perhaps, cancelable biometrics (Bolle, Connell, & Ratha, 2002). Additionally organizational practices and activities should be geared towards optimizing privacy protections.

Very recently, a government-commissioned report on identity assurance prepared by Sir James Crosby included in its ten broad principles for consumer-driven universal ID assurance the following recommendation, which speaks to the arguments of this paper: "As a matter of principle, the amount of data stored should be minimised. **Full biometric images (other than photographs) should not be kept. Only non-unique digital representations of biometric images should be stored**. Additional data accessed during enrolment and records of verification enquiries should not be retained. All data and systems should be protected by 'state of the art' encryption technology" (Crosby, 2008, p. 7, emphasis added).

Time will tell whether those in charge of the NIR and its development take heed of this recommendation. In any case, it should be reiterated that regulating something like privacy in such multifold ways is tremendously difficult, which calls into question the advisability of mass government collection of biometrics.

6. Conclusion

To be fair, the Home Office and Identity and Passport Service have taken some small strides to address arguments like those outlined above. The National Identity Scheme Delivery Plan states, "We will consult with the Information Commissioner on the information we will hold on the NIR. Our aim is to have the minimum information on the NIR needed to identify an individual and to meet the statutory purposes under the Identity Cards Act 2006" (UKIPS, 2008, p. 13). This appears an attempt to address issues of proportionality and, perhaps indirectly, secondary use. Unfortunately, history shows that regulatory bodies like the Information Commissioner's Office have limited powers to make good on extensive policy protections.

This paper has deliberated on the ways privacy concerns related to proportionality and secondary uses of data are implicated by the proposed UK NIR. There are, however, numerous other components of privacy that also deserve a focused analysis. Scope limitations have prevented such analyses in this undertaking and further research is necessary. For example, as concerns highly sensitive biometric information stored on the register, there is the potential for blackmail by those with insider access. If such information were to reveal a serious medical condition, the disclosure of which proving devastating to the data subject, then there is a case to be made that there is real harm to be done. Blackmail is just one such privacy area that remains to be explored.

Beyond the privacy debate, however, there are numerous other issues related to the public perceptions of and confidence in government systems that demand further academic scrutiny, not just in the UK but all over the globe. With biometrics being incorporated into various identity systems internationally, be they at airports, land border crossings or as part of local entitlement schemes, for example, the public are increasingly encountering systems involving high degrees of technological complexity and innovation. Researchers need to begin asking questions about the ways in which the public interpret and make sense of such innovative systems. Arguably, public reactions to, understandings of and trust in such biometric innovations will largely determine their uptake and success.

Acknowledgements

The author would like to thank Drs. Gus R. Hosein, Matthew L. Smith and Edgar A. Whitley, and Ms. Caitlin M. Connors, for their extensive feedback.

References

Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric perils and patches. Pattern Recognition, 35(12), 2727-2738.

Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008). Image understanding for iris biometrics: A survey. Computer Vision and Image Understanding, In Press, Corrected Proof.

Buchanan, K. (2007). DNA 'will be stolen' from ID cards. Retrieved 4 March, 2007, from http://personal.lse.ac.uk/martinak/DNA.pdf

Clarke, R. A. (1998). Smart Card Technical Issues Starter Kit. Retrieved March 10, 2008, from http://www.anu.edu.au/people/Roger.Clarke/DV/SCTISK.html

Clarke, R. A. (2001, 15 April 2001). Biometrics and Privacy. Retrieved 9 December, 2006, from http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

CNN. (2007). Experts warn of identity theft risk. Retrieved 4 April, from http://edition.cnn.com/2007/TECH/ptech/03/14/photocopier.risks.ap/index.html

Crosby, J. (2008). Challenges and opportunities in identity assurance. London: HM Treasury.

Davies, S. (1998). Biometrics - A Civil Liberties and Privacy Perspective. Information Security Technical Report, 3(1), 90-94.

Espiner, T. (2007). MP: ID card scheme is 'doomed to failure'. ZDNet.co.uk Retrieved 2 April, 2007, from http://news.zdnet.co.uk/security/0,1000000189,39285467,00.htm

EU Directive. (1995). 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the EC, 23.

Faundez-Zanuy, M. (2004). On the vulnerability of biometric security systems. Aerospace and Electronic Systems Magazine, IEEE, 19(6), 3-8.

Faundez-Zanuy, M. (2005). Privacy issues on biometric systems. Aerospace and Electronic Systems Magazine, IEEE, 20(2), 13-15.

Genewatch. (2006). The DNA Expansion Programme: reporting real achievement?

HMIC. (2000). HMA v Shirley McKie. from http://www.scotland.gov.uk/hmic/docs/fppi-15.asp

Identity Cards Act. (2006). from http://www.opsi.gov.uk/acts/acts2006/plain/ukpga_20060015_en_1

Jain, A. K., & Ross, A. (2004). Multibiometric systems. Communications of the ACM, 47(1), 34-40.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

Jones, L. A., Antón, A. I., & Earp, J. B. (2007). Towards understanding user perceptions of authentication technologies. Paper presented at the Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society.

Lazarick, R. (2005). Multibiometric techniques and standards activities. Paper presented at the 39th Annual 2005 International Carnahan Conference on Security Technology.

Lessig, L. (1999). Code and Other Laws of Cyberspace. New York, NY, USA: Basic Books.

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of Artificial Gummy Fingers on Fingerprint Systems. Proceedings of SPIE, 4677(1), 275-289.

Nisenson, M., Yariv, I., El-Yaniv, R., & Meir, R. (2003). Towards Behaviometric Security Systems: Learning to Identify a Typist. Lecture Notes in Computer Science, 2838, 363-374.

O'Gorman, L. (2003). Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings- IEEE, 91(12), 2021-2040.

Qiu, X., Sun, Z., & Tan, T. (2006). Global texture analysis of iris images for ethnic classification. Paper presented at the International Conference on Biometrics.

Schwartz, P. (1999). Privacy and Democracy in Cyberspace. Vanderbilt Law Review, 52(6), 1610-1702.

Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review, 154, 477-564.

Thomas, V., Chawla, N., Bowyer, K., & Flynn, P. (2007). Learning to predict gender from iris images. Paper presented at the Biometrics: Theory, Applications, and Systems.

UKIPS. (2006). Strategic Action Plan for the National Identity Scheme: Safe guarding your identity. from http://www.identitycards.gov.uk/downloads/Strategic_Action_Plan.pdf

UKIPS. (2008). National Identity Scheme Delivery Plan. from http://www.ips.gov.uk/identity/downloads/national-identity-scheme-delivery-2008.pdf

Zorkadis, V., & Donos, P. (2004). On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements. *Information Management & Computer Security, 12*(1), 125-137.

Zviran, M., & Erlich, Z. (2006). Identification and Authentication: Technology and Implementation Issues. Communications of the Association for Information Systems, 17(4), 90-105.