

# 13 From surveillance-by-design to privacy-by-design

## Evolving identity policy in the United Kingdom

*Edgar A. Whitley, Aaron K. Martin and Gus Hosein*

### 13.1 Introduction

Few artefacts capture the history of surveillance better than an identity card. In fact, the process of establishing identity predates the card, where throughout history the registration of individuals was associated with citizenry (e.g. Pharaonic Egypt), imperialism (e.g. Rome's census in Palestine) and ownership (e.g. William the Conqueror's Domesday Book). Over time, portable documents held by citizens replaced the use of central registers (Torpey 2000).

With the rise of the nation state, identity cards became increasingly commonplace. So did identity checks. The query of 'your papers, please' now captures the public imagination as a key form of abuse of the powers of the state. This is particularly the case in countries that never established a long-standing identity card apparatus, including much of the English-speaking world and, of course, the United Kingdom (UK).

To many, identity policy is seen to be quite simple and a mere bureaucratic necessity. In reality, modern identity policy involves a complex socio-technical system. That is, an identity policy relies intensely upon technology, while it also alters the relationship between the individual and the state (Whitley and Hosein 2010b). This is not always a negative development, and, in fact, identity policy can be both empowering and protective while meeting the needs of state administration. At other times, however, the policies proffered may interfere with rights, rely on unstable or unreliable technologies, involve significant costs, introduce problematic politics and accomplish few of the stated objectives.

When the UK government proposed reintroducing an identity card in the early 2000s it was seeking to respond to administrative imperatives, but also to address pressing policy issues, including terrorism, crime, immigration and fraud. It sought to solve all these problems with a complex socio-technological system in a form that the world had not previously seen. It quickly developed a momentum that made it appear as though nothing could prevent the scheme from becoming a reality. It took significant countervailing forces, some intentional and some accidental, to disrupt the dominant narrative. This chapter presents how the latest attempt at introducing a UK identity card became part of history, rather than a determinant of the future of British society and governance.

### 13.2 A prehistory

The former UK government's proposals for identity cards were not the first instance of an identification programme in the country. During both the First and Second World Wars, Britain introduced a form of national identity card.

According to Agar (2005), the first-ever attempt at a national identity card and population register in the UK was a failure. The programme was introduced during the First World War as a means of determining the extent of the male population in the country. Existing government records were considered incomplete and ineffective for the purposes of developing a policy for conscription. Once the count was completed and the government knew how many men were available to serve, political interest in national registration and identification cards waned and the system was soon abandoned.

However, as Agar notes, the promise of a national identification system was not forgotten by the Civil Service, which during the Second World War reintroduced the idea of identity cards, primarily as a way of identifying aliens and managing the allocation of food rations.

Crucial to the operation of the second National Register was its intimate connection to the organisation of food rationing. In order to renew a ration book, an identity card would have to be produced for inspection at a local office at regular intervals. Those without an identity card, would within a short period of time no longer be able, legally, to claim rationed food. This intimate connection between two immense administrative systems was vital to the success of the second card – they were not forgotten by members of the public – and provides one of the main historical lessons.

(Agar 2005)

As identity cards became a facet of everyday life, they started being used for additional purposes (i.e. they were subject to 'function creep'), including identity checks by police officers. This use continued even after the war was over. Liberal-minded citizens eventually began to question these practices and, in 1950, one such citizen, Clarence Willcock, disputed the police's routine check of identity cards. Willcock's legal challenges were not successful, but in the case's written judgment Lord Goddard (the Lord Chief Justice) criticized the police for abusing identity cards. By 1952 Parliament had repealed the legislative basis for the national identity card and it disappeared from use.

### 13.3 The case of the national identity scheme: innovations in technology, identification and surveillance

As many observers have noted, including civil society groups (Privacy International 1997), the Civil Service and politicians have since been regularly captivated by the idea of reintroducing national identity cards in the UK with the aim of solving a diversity of policy problems, ranging from streamlining tax

1 administration to ‘fixing’ the immigration ‘problem’, among others. By the early  
2 2000s they had tried again.

3 In 2002, the Labour government, under Prime Minister Tony Blair and with  
4 David Blunkett serving as Home Secretary, proposed a new national ‘entitlement  
5 card’ scheme. This proposal was then rebranded as a national ‘identity card’  
6 scheme in 2004. Following failed attempts to pass the legislation, as well as a  
7 general election in the UK (in which the Labour Party was again re-elected to  
8 government) and a political and constitutional crisis in which the Upper  
9 Chamber (the House of Lords) kept returning the Bill back to the Lower  
10 Chamber (the House of Commons) due to various concerns, Parliament passed  
11 the Identity Cards Act 2006 on 30 March, thus enabling the first national identity  
12 card programme since the Second World War. By this point it had become a  
13 contentious piece of legislation, particularly on grounds of costs, technological  
14 feasibility and civil liberties.

15 This new scheme was different from previous ones in several important ways.  
16 The proposals called for a system of unprecedented size and complexity, com-  
17 prising a centralized National Identity Register (the electronic database on which  
18 the population’s identity data would be held) and the collection and recording of  
19 over 50 pieces of personal information from individuals, including most notably  
20 the collection and use of the biometric information on UK citizens and residents.

21 Moreover, a number of features distinguished this scheme from those in other  
22 countries. These features included the extensive use of biometrics both for enrol-  
23 ment (to ensure that no individual was entered in the Register more than once)  
24 and verification, the proposed use of a single identification number across gov-  
25 ernment and the private sector (Oti Jacques *et al.* 2007), and an ‘audit trail’ that  
26 was expected to record details of every instance when an identity was verified  
27 against information stored on the Register.<sup>1</sup> Many argued that this was  
28 surveillance-by-design because of the extensive collection and use of personal  
29 information being proposed, as well as the expansive purposes for which the  
30 system would be used.

31 The successful implementation of the scheme would have required consider-  
32 able organizational resources: technological expertise in the development of  
33 large-scale, secure databases, advanced computer chip technologies for ‘smart’  
34 identity cards, arduous registration processes involving physical interaction with  
35 each resident thereby requiring office space and mobile registration facilities,  
36 sophisticated data-collection mechanisms to check people’s ‘biographical foot-  
37 print’ during the enrolment process, system integration skills to combine all the  
38 different aspects of the scheme, and specialist skills in biometric enrolment and  
39 verification.

40 Even after the difficulties and modifications to the programme during the  
41 legislative phase, the government’s programme for identity cards went through  
42 various transformations after the Bill became law. The configuration of the  
43 National Identity Register, for example, underwent several changes. In its ori-  
44 ginal conception, the Register was to be a brand-new, central store of data. The  
45 purpose of a new database was to ensure that there were no errors or fraudulent

identities being propagated into the new system. This changed in December 2006 when the Identity and Passport Service (UKIPS) – the sub-department of the Home Office responsible for implementing the scheme – released its *Strategic Action Plan* and set out a revised database schema for the Register. The idea was to separate the biographic, biometric and administrative information data and store them on different (logical) databases. The stated reasons for this segregation were to improve security and make use of “the strengths of existing systems” (UKIPS 2006: 10); however it could also be perceived as an attempt to reduce costs by reusing information and reducing resources.

The contentious aspects raised during the legislative process continued to affect the scheme as it moved into the development and implementation phases. In turn, the government’s proposals for identity cards went through various other changes over the course of the scheme’s life span, primarily motivated by concerns about managing costs and achieving observable successes to convince the public, industry, other government agencies and critics.<sup>2</sup>

### 13.4 A history of biometrics in the scheme

Of particular interest to the history of surveillance is the biometrics component of the scheme – the government’s proposals for these technologies were visionary if not audacious. The collection of multiple biometrics, including digital facial photographs, fingerprints, irises and signatures, from tens of millions of citizens and foreigners (under a separate but related piece of legislation, the UK Borders Act 2007 (Warren and Mavroudi 2011)) had not been undertaken before as part of a national identity system. Another significant innovation was the plan for real-time, online biometric identification against a centralized, government-managed database. While other countries already operated their own national identity systems, the proposed use of these biometrics in this way – and on this scale – was something that had not been attempted before (Martin 2012).

Yet the history of biometrics in the scheme was, in a way, rather ambiguous and irregular. The government’s plans for biometrics were never fully explicit or certain. For example, when the Labour government first proposed entitlement cards in a 2002 consultation paper, the use of biometrics was considered simply an ‘option’ within a much larger proposal for the entitlement cards scheme. The inclusion of biometrics was said to be ultimately dependent on the feasibility, cost-effectiveness and, importantly, public acceptance of the Home Office’s proposals (Home Office 2002: 2).

Eventually biometrics became a key requirement of the proposed scheme, enshrined in the Identity Cards Act 2006, where the Prime Minister even justified the introduction of identity cards on the grounds that biometrics were now possible to process at this scale (Blair 2006). Throughout, however, the specifics around biometrics in the scheme would remain fuzzy. For example, the decision about which biometrics the government would use to identify citizens was never firm. It was deliberately technology neutral. While facial photographs were always considered the most viable and practicable option, they were not always

1 spoken about as ‘biometric’ and instead were sometimes treated differently,  
2 partly due to the fact that they were not perceived as particularly hi-tech as com-  
3 pared to other available technologies.

4 Digital fingerprinting, the most publicly recognizable biometric technology,  
5 was also subject to uncertainty in the government’s plans. For example, the ori-  
6 ginal thinking was to collect only four fingerprints from citizens. However, the  
7 number of fingerprints to be scanned was increased to ten – a policy decision  
8 that seemed as certain as any in the scheme until a leaked government document,  
9 made public by the campaign group No2ID,<sup>3</sup> revealed that the apparently settled  
10 policy for everyone to enrol all ten fingerprints was not necessarily set in stone.  
11 In a bullet point in the ‘Options Analysis’ document, unnamed decision-makers  
12 conceded that the “nature of the group(s) selected drives the requirement for the  
13 [biometrics] infrastructure (especially face vs. fingerprints)” (NO2ID 2008: 2).  
14 That is, the Home Office was considering the option of allowing certain social  
15 groups to avoid fingerprint enrolment. No2ID interpreted this disclosure as an  
16 “indication that dropping fingerprints is being considered for some groups. This  
17 blows apart the government’s whole case for the identity scheme, which rests on  
18 ‘biometrically securing’ personal information and preventing multiple/fraudulent  
19 applications through biometric cross-checking” (see NO2ID’s annotations in  
20 NO2ID 2008: 2).

21 Government officials regularly described iris biometrics as a future option  
22 because of its potential for uniquely identifying large populations, thus again  
23 providing a means for preventing multiple or fraudulent identities (Martin and  
24 Whitley 2013). Despite extensive claims in the parliamentary debate around the  
25 virtues of iris biometrics, the technology was never guaranteed to feature in the  
26 national identity scheme. This was despite many bold claims made by officials  
27 about what the programme was supposed to achieve – claims which many  
28 experts agreed were impossible without incorporating robust and scalable tech-  
29 nology such as iris biometrics from the outset. For example, claims about  
30 effective one-to-many biometric searches using fingerprint records in a fully  
31 populated identity database were deemed far-fetched by experts, who argued that  
32 only iris biometrics were capable of performing on this scale (see e.g. the per-  
33 spective of Professor Daugman in BBC News (2007)).

34 A final policy change relating to biometrics was the decision by the Home  
35 Office not to enrol biometrics in-house – that is, by establishing government-run  
36 registration offices across the country for people to come and submit their bio-  
37 metrics in exchange for a new identity card – but rather to look to the market for  
38 ways of outsourcing this function. This decision, publicized in 2008, was an  
39 apparent attempt to reduce the cost to the Home Office of recording people’s  
40 biometrics, with the idea being that people would pay out-of-pocket to enrol  
41 their biometrics at high street locations such as the post office or pharmacies.  
42 This move to the market was never completed because the scheme was scrapped  
43 before the contracting processes were finalized. Still, the desire to seek out exter-  
44 nal organizations to assist with biometric enrolment represents an important  
45 event in the history of the identity card.

### 13.5 Politics, trust and public perception

It is also important to highlight the broader political developments that affected the scheme. Following the 2005 election, the leader of the opposition Conservative Party resigned. Michael Howard had been a strong proponent of identity cards when his party was in power and as Home Secretary he had also considered (but did not implement) a national identity card in the mid-1990s. Thus, when the Identity Cards Bill went through the House of Commons in late 2004 and early 2005, the opposition party did not make a concerted effort to fight it. In one famous moment, rather than vote for or against a version of the Bill at one stage in Parliament, he ordered the Members of Parliament from his party to ‘go Christmas shopping’, i.e. to absent themselves from the vote.

When Mr Howard announced that he was stepping down as leader of the Conservative Party, other members of the party began voicing stronger opposition to Labour’s proposals for national identity cards. The Conservative Party’s leadership contest ended up being between two strong opponents to the Bill: David Cameron (who, as a member of the Home Affairs Committee that had looked into the Bill, had previously spoken about his unhappiness with the policy, particularly the way it changed the relationship between the citizen and the State (Cameron 2004)), and David Davis (who was appointed as the lead member of the Opposition on the Bill in the Commons). With Cameron’s election as party leader the Conservative Party position on the Bill became stronger. In one of his first interviews as party leader, he articulated his concerns about the Bill. Meanwhile, the third party of British politics, the Liberal Democrats, consistently held strong beliefs that the Bill was contrary to civil liberties.

In June 2005, a research group based at the London School of Economics (of which the authors of this chapter were an integral part) issued a detailed report that critically analysed the government’s proposals (LSE Identity Project 2005). The LSE researchers suggested that the likely cost of the scheme was far higher than government estimates, evaluated the likely technology solutions and challenges in deploying these technologies, and identified focal points around the policy that would likely give rise to privacy and surveillance concerns. This led to widespread media coverage around these lines of criticism and most notably the costs of the scheme; while the parliamentary debate was fuelled by data and analyses from the LSE report.

Even once Parliament had formally approved the scheme and created the new Identity and Passport Service from the previous Passport Agency, the government’s plans did not run smoothly. In July 2006, leaked emails from senior civil servants warning about ongoing risks to the scheme were published on the front page of a major newspaper (*The Sunday Times* 2006). Shortly thereafter, the new Home Secretary (the third in as many years and the third overseeing this policy) ordered a wholesale review of the plans for the scheme given worries that many parts of his department were ‘not fit for purpose’. This review resulted in the *Strategic Action Plan* issued in December 2006 (UKIPS 2006) that sought to reduce the risks and costs of the scheme.

1 Another significant event that affected the government's plans was the  
2 announcement by the then Chancellor Alistair Darling, on 20 November 2007,  
3 that a data breach involving "personal data relating to child benefit" had arisen  
4 in Her Majesty's Revenue and Customs (HMRC) (20 November 2007: Column  
5 1101–). On 18 October 2007, in response to a request from the National Audit  
6 Office (NAO) for data in relation to payment of child benefit, a civil servant at  
7 HMRC sent a full copy of the data on two password-protected compact discs,  
8 using an obsolete version of compression software with weak encryption. The  
9 discs were sent using the HMRC's internal mail service, operated by TNT. The  
10 package was not recorded or registered and failed to arrive at the NAO. When  
11 the requested discs did not arrive, a second set of discs was sent, this time by  
12 recorded delivery. These did arrive.

13 The original discs, containing details of all child benefit recipients – records  
14 for 25 million individuals and 7.25 million families – have still not been  
15 recovered. The records included the names of recipients as well as their children,  
16 address details and dates of birth, child benefit numbers, national insurance  
17 numbers and, where relevant, bank or building society account details.

18 Unsurprisingly, public trust in the government's ability to keep personal data  
19 secure was negatively affected by this news and the implications for the National  
20 Identity Scheme were widely reported. In addition, because of a parliamentary  
21 requirement for the scheme to report on costs every six months (negotiated at the  
22 final stages to permit the Bill to be approved by Parliament after the constitu-  
23 tional crisis to which it had given rise), the government's plans retained a far  
24 higher public profile than most e-government projects.

25 Detailed qualitative analysis of the press coverage of the scheme (Pieri 2009)  
26 reveals that this coverage was overwhelmingly negative. In particular, media  
27 coverage emphasized the many risks and problems the scheme was facing. This  
28 negative coverage was particularly significant, as it appeared alongside  
29 government-issued press releases that sought to highlight the benefits of the  
30 scheme to citizens and government alike.

31 With public opinion potentially playing such a leading role in the eventual  
32 success of the scheme, both the Home Office and No2ID conducted a series of  
33 opinion polls about public perceptions of identity cards.

34 The Home Office commissioned a series of studies examining public attitudes  
35 to the National Identity Scheme and identity cards by the Central Office of  
36 Information (UKIPS 2008). Six studies took place (February 2007, October  
37 2007, January/February 2008, May 2008, August 2008 and November 2008) and  
38 involved adding questions to a general public omnibus survey. The questions  
39 were intended to elicit awareness and attitudinal data about identity cards and  
40 the scheme, and the questions covered topics such as awareness of identity cards,  
41 support for the programme, the reasons for introducing the identity system and  
42 proposed benefits (Whitley 2009). Support for the scheme in these samples  
43 remained statistically stable at around 60 per cent.

44 No2ID also organized a series of public opinion polls that it commissioned  
45 from ICM research. Its research asked the same question over time, namely:

‘The government has proposed the introduction of identity cards that, in combination with your passport, will cost around £93. From what you have seen or heard do you think that this proposal is a ... [good ... bad idea]?’ In contrast to the Home Office-sponsored research, this stream shows a decline in the net scores for the identity card scheme being ‘a good idea’, down from 81 per cent in December 2004 to less than 50 per cent in June 2008, with a sustained drop following the HMRC data breach.

### 13.6 A trust deficit in a surveillance state

The surveys by No2ID and the Home Office demonstrated low levels of trust in the government’s plans to implement identity cards. In the run-up to the 2010 general election, opposition parties in the UK began to articulate the basis of their concerns with the government’s identity policy as embodied in the National Identity Scheme and to build on the falling support for the government’s plans. For the Conservative Party, the identity card scheme became part of a broader narrative that presented the government’s policy as creating a surveillance state, a policy that needed to be reversed (Conservatives 2009). This reversal began with the belief that personal information belongs to the citizen, not the state, and where the government collects private details they are held on trust. As a result, the conservative logic was that the government must be held accountable to its citizens, not the other way around (Conservatives 2009).

In their election manifesto, this goal of introducing measures “to protect personal privacy and hold government to account” became an espoused part of the Conservative Party policy agenda, under the heading “Protect our freedoms”:

Labour’s approach to our personal privacy is the worst of all worlds – intrusive, ineffective and enormously expensive. We will scrap ID cards, the National Identity Register and the Contactpoint database.

(Conservative Party 2010)

The third major political party, the Liberal Democrats, also reiterated its long-standing opposition to identity cards. Their manifesto noted that:

increasing use of sophisticated technology, whilst bringing undoubted benefits to society, also poses new threats to individual liberty, particularly in relation to Identity Cards. The Liberal Party opposes the introduction of any form of national Identity Card, whether voluntary or compulsory.

(Liberal Democrats 2010)

By the time of the general election, every political party other than the Labour Party had included proposals to scrap identity cards as part of their election manifestos.

In the 2010 election, no single party won an overall majority and, after a period of negotiation and speculation about whether one party might try to



1 operate a minority government, a coalition between the Conservative and Liberal  
2 Democrat parties was announced. Perhaps unsurprisingly, a key feature of the  
3 joint ‘Coalition Agreement’, announced on 11 May 2010, was plans:

4  
5 to implement a full programme of measures to reverse the substantial  
6 erosion of civil liberties under the Labour Government and roll back state  
7 intrusion. This will include:

- 8
- 9 • A Freedom or Great Repeal Bill
- 10 • The scrapping of ID card scheme, the National Identity register, the  
11 next generation of biometric passports and the Contact Point Database.

12 (Conservative Liberal Democrat coalition negotiations 2010)  
13

14 The first piece of legislation introduced by the new Coalition Government (“Bill  
15 1 of 2010–11”) was the “Identity Documents Bill”, which was “A Bill to make  
16 provision for and in connection with the repeal of the Identity Cards Act 2006”.  
17 Passage of the Bill took longer than the government had anticipated (not least  
18 because of concerns raised by the Labour Party about possibly compensating  
19 those citizens who had paid for identity cards that were about to be revoked – by  
20 May 2010 14,670 cards had been issued). The Bill received Royal Assent on 21  
21 December 2010, at which point identity cards ceased to have legal status. On 10  
22 February 2011, Home Office minister Damian Green marked the end of the identity  
23 card scheme by feeding its drives into an industrial shredder in Essex (Mathieson  
24 2011).

25 While scrapping the unloved national identity scheme and even physically  
26 grinding to dust key hardware components of the system provides an important  
27 symbolic moment in the short history of a surveillance-led identity policy, it  
28 does not resolve questions of how individuals can feasibly identify themselves in  
29 order to gain access to services. The challenge of an effective identity policy  
30 does not go away with a new government. In particular, government services  
31 still need to have confidence in the people with whom they are interacting, and  
32 citizens need to have trust in the identity system they must use to interact with  
33 government.  
34

### 35 **13.7 Realigning trust, policy and technology**

36  
37 When the Identity Documents Bill was introduced to Parliament at Second  
38 Reading, Home Office Minister Damian Green emphasized the role the Bill was  
39 playing in repairing trust:  
40

41 Scrapping the ID card scheme shows the clear intent of the coalition Gov-  
42 ernment to roll back the intrusion of the state and to return personal freedom  
43 and control to the individual citizen. This Bill is a major step on that road.  
44 Bringing the Bill before the House at such an early stage of the new Gov-  
45 ernment signifies the importance that we place on creating a free society and

on cutting unnecessary expenditure. *The Bill is also about trust*. It is about the people having trust in the Government to know when it is necessary and appropriate for the state to hold and use personal data and it is about the Government placing their trust in the common-sense and responsible attitude of the people. The previous Government's ID cards scheme and the national identity register, which lay at its heart and which was its most reprehensible part, failed on both counts.

(9 June 2010: Column 429; emphasis added)

As such, scrapping the existing identity card scheme was an important first step in repairing the trust lost between the citizen and the State. It acknowledges that trust was lost due to explicit policy choices made by the previous government (Gillespie and Dietz 2009). As such, it contrasts with the findings of many studies in which trust is lost because of the actions of rogue individuals or the failure of appropriate oversight and governance mechanisms (Colquitt and Rodell 2011).

As a result, more traditional trust responses such as external governance in the form of legislation and other regulatory mechanisms are unlikely to restore public trust precisely because the loss of trust arose due to a particular previous choice of legislation and other regulatory mechanisms.

Scrapping identity cards does, however, provide a starting point for rebuilding trust, echoing the first stage ("immediate response") of Gillespie and Dietz's (2009) four-stage process of organization-level trust repair. Their second stage, "diagnosis", was also found in the various election statements of the coalition partners – "personal information belongs to the citizen, not the state"; "increasing use of sophisticated technology . . . poses new threats to individual liberty".

Indeed, a key element of the diagnosis can be traced back to a critical report written by an external adviser to the UK Treasury, Sir James Crosby (2008). Sir James was appointed by the then Chancellor Gordon Brown, who was believed to be critical of his own party's policy on identity cards. Crosby's report could have allowed Brown to restructure his government's identity policies upon (eventually) taking over as Prime Minister from Tony Blair.

Crosby's report focused the issue away from 'ID cards' and the arising 'identity management' discourse and instead referred to 'identity assurance'. His choice of terminology was deliberate. The final report notes that:

At an early stage, we recognised that consumers constitute the common ground between the public and private sectors. And our focus switched from 'ID management' to 'ID assurance'. The expression 'ID management' suggests data sharing and database consolidation, concepts which principally serve the interests of the owner of the database, for example the Government or the banks. Whereas we think of 'ID assurance' as a consumer-led concept, a process that meets an important consumer need without necessarily providing any spin-off benefits to the owner of any database.

(Sir James Crosby 2008: 3)

1 Crosby believed that the distinction was fundamental, as an identity policy “built  
2 primarily to deliver high levels of assurance for consumers and to command  
3 their trust has little in common with one inspired mainly by the ambitions of its  
4 owner” (Sir James Crosby 2008: 3).

5 Acknowledging past mistakes (even those that can be blamed on previous  
6 ministers, officials or government) might help regain the trust citizens have when  
7 interacting with government. However, a second trust relationship is implicated  
8 in an identity policy, namely that of the state trusting the citizen, and for this  
9 further work is required. Moreover, the design of the reforming interventions  
10 (Gillespie and Dietz 2009) is constrained by the consequences of earlier parts of  
11 the trust repair process. The coalition government is constrained by the decisions  
12 to scrap the national identity scheme and not to rely on large-scale centralized  
13 databases of citizen information held and potentially monitored by the State. The  
14 next section therefore describes how the government’s identity assurance pro-  
15 gramme seeks to enable trusted online transactions that regain citizen trust in the  
16 UK government’s identity policy.

### 18 **13.8 Identity assurance in the UK: 2010 to the present**

19 The government’s identity assurance programme provides a radically different  
20 solution to the question of how the State can trust the identity claims of its  
21 citizens. Given the policy decision not to rely on centralized databases of citizen  
22 data and the avowed approach to make identity policy benefit the citizen in the  
23 first instance, the government’s trust repair processes involve a complex inter-  
24 play of institutional perspectives on risk, citizen-centric approaches to data man-  
25 agement and technological measures to ensure that citizen trust is upheld.

26 In terms of institutional perspectives on trust and risk, the previous govern-  
27 ment’s identity policy was based on trusting a “gold standard of identity” (Bar-  
28 oness Scotland, 16 November 2005, Column 1167) in the form of relying on the  
29 details stored on the National Identity Register. In contrast, the identity assur-  
30 ance programme’s alternative mechanism is based on the decision to take a  
31 transactional viewpoint of services based on distributed delivery models (Cabinet  
32 Office 2012a). This alternative approach to the secure delivery of online public  
33 services (Cabinet Office 2012a) has two key features. First, it explicitly empow-  
34 ers risk owners in government to make risk-based assessments about all aspects  
35 of the process. That is, rather than providing a single, biometric-based solution  
36 for all government identity claims, the new approach encourages each govern-  
37 ment department to make its own risk-based decision about what identity evi-  
38 dence it will accept. The second feature of the approach is the acceptance of  
39 distributed delivery mechanisms. In particular, this means that the government  
40 recognizes that there may be a range of different identity credentials that could  
41 be used to access government services. In order to make this process manageable  
42 for all parties, the Cabinet Office is adopting a guiding role in specifying a range  
43 of risk options from which government departments can choose, using its techni-  
44 cal expertise to ensure that identity credential providers can be trusted to deliver  
45

services at levels of assurance that match the possible risk options chosen by government departments (Cabinet Office 2013). This approach allows government to benefit from economies of scale while providing a standard marketplace for identity services – a marketplace that the government has vowed not to enter as an identity provider.

In this way, rather than having individual government departments building their own individual identity systems or requiring all government departments to rely on a single point of trust about identity claims, the new approach requires departments to make a risk-based assessment of the level of assurance it requires for its identity claims (thus, an identity claim to request information about public services is likely to require a different level of assurance to an identity claim about receiving social security benefits). A market of identity providers will then offer credentials to citizens that support different levels of assurance and hence allow access to different government services.

Given the concerns about government creating a surveillance society, a key feature of the technological implementation of the identity assurance programme is the use of sophisticated cryptographic techniques. These techniques enable the reliable use of identity credentials to access government services without the identity provider knowing which government service the citizen is using (to prevent private sector surveillance of government interactions) and without the government service knowing which identity provider was supporting the particular identity claims (to avoid similar government-based tracking of individuals).

A third distinctive feature of the identity assurance programme is the central role played by a specially formed Privacy and Consumer Advisory Group. This group, consisting of key members of civil society with an interest in identity policy including No2ID, academics including researchers from the London School of Economics, consumer groups and regulators (namely the Information Commissioner's Office), has developed a series of citizen-focused privacy principles (Cabinet Office 2012b). These principles are being used to guide the activities of recently appointed identity providers so that the identity assurance programme regains the trust of citizens in the new identity policy.

### 13.9 Conclusions

While the outcomes of this new policy direction are still unknown, the episode of the national identity scheme shows that surveillance technology developments are not inevitable – that resistance (Martin *et al.* 2009) and policy redirection are not mere theoretical possibilities, but achievable in practice. The short-lived history of the latest iteration of national identity cards in the UK is an important story of government surveillance aspirations and policy failure in which the vision of a nationwide biometric identity system proved not to be a foregone conclusion. Tony Blair was gravely mistaken when he argued that identity cards “were an idea whose time has come” (*Daily Telegraph* 2005), at least for the UK. History has clearly proven otherwise. We hope that this history inspires others to engage similarly problematic policies, across Europe and beyond.

## Notes

- 1 This requirement for a personal audit trail would prove to be particularly controversial among activists, who viewed it as a dangerous tracking device.
- 2 For a more extensive history of the national identity scheme see Whitley and Hosein (2010a: chs 3–4).
- 3 No2ID is an independent campaigning organization opposed to identity cards and “the database state”.

## References

- Agar, Jon. 2005. Identity cards in Britain: past experience and policy implications. *History and Policy*. Archived at: [www.historyandpolicy.org/papers/policy-paper-33.html](http://www.historyandpolicy.org/papers/policy-paper-33.html).
- BBC News. 2007. ID cards will give ‘false’ data. BBC. Available at: [http://news.bbc.co.uk/1/hi/programmes/file\\_on\\_4/6922882.stm](http://news.bbc.co.uk/1/hi/programmes/file_on_4/6922882.stm) (accessed 5 November 2010).
- Blair, Tony. 2006. We need ID cards to secure our borders and ease modern life. Available at: [www.telegraph.co.uk/comment/personal-view/3633979/We-need-ID-cards-to-secure-our-borders-and-ease-modern-life.html](http://www.telegraph.co.uk/comment/personal-view/3633979/We-need-ID-cards-to-secure-our-borders-and-ease-modern-life.html).
- Cabinet Office. 2012a. Good Practice Guide 43: Requirements for Secure Delivery of Online Public Services (April). Archived at: <https://update.cabinetoffice.gov.uk/sites/default/files/resources/GPG43-RSDOPS-issue-1-0-April-2012.pdf>.
- Cabinet Office. 2012b. Good Practice Guide 45: Validating and Verifying the Identity of an Individual in Support of HM Government Online Services (April). Archived at: <https://update.cabinetoffice.gov.uk/sites/default/files/resources/GPG-45-validating-and-verifying-the-identity-issue-1.0-April-2012.pdf>.
- Cabinet Office. 2013. Good Practice Guide 45: Identity Proofing and Verification of an Individual (May). Archived at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/204448/GPG\\_45\\_Identity\\_proofing\\_and\\_verification\\_of\\_an\\_individual\\_2.0\\_May-2013.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204448/GPG_45_Identity_proofing_and_verification_of_an_individual_2.0_May-2013.pdf).
- Cameron, David. 2004. Mistaken Identity: A Public Meeting on the Government’s Proposed National Identity Card (19 May). Archived at: [www.no2id.net/MistakenIdentity/Mistaken\\_Identity\\_05.mp3](http://www.no2id.net/MistakenIdentity/Mistaken_Identity_05.mp3).
- Colquitt, Jason and Jessica Rodell. 2011. Justice, trust and trustworthiness: a longitudinal analysis integrating three theoretical perspectives. *Academy of Management Journal* 54(6): 1183–1206.
- Conservative Liberal Democrat coalition negotiations. 2010. Agreements reached (11 May).
- Conservative Party. 2010. Manifesto: Invitation to Join the Government of Britain.
- Conservatives. 2009. Reversing the Rise of the Surveillance State: 11 Measures to Protect Personal Privacy and Hold Government to Account. Archived at: [www.conservatives.com/News/News\\_stories/2009/09/~~/media/Files/Policy%20Documents/Surveillance%20State.ashx](http://www.conservatives.com/News/News_stories/2009/09/~~/media/Files/Policy%20Documents/Surveillance%20State.ashx).
- Daily Telegraph. 2005. Time Has Come for ID Cards, says Blair. *Daily Telegraph* (28 June). Archived at: [www.telegraph.co.uk/news/1492875/Time-has-come-for-ID-cards-says-Blair.html](http://www.telegraph.co.uk/news/1492875/Time-has-come-for-ID-cards-says-Blair.html).
- Gillespie, Nicole and Graham Dietz. 2009. Trust Repair after an Organization Level Failure. *Academy of Management Review* 34(1): 127–145.
- Home Office. 2002. Entitlement Cards and Identity Fraud: A Consultation. Paper. Stationery Office. Available at: [www.privacyinternational.org/documents/idcard/uk/entitlementcard-consultation.pdf](http://www.privacyinternational.org/documents/idcard/uk/entitlementcard-consultation.pdf).

218 E.A. Whitley et al.

- Liberal Democrats. 2010. Manifesto 2010. Archived at: [http://network.libdems.org.uk/manifesto2010/libdem\\_manifesto\\_2010.pdf](http://network.libdems.org.uk/manifesto2010/libdem_manifesto_2010.pdf).
- LSE Identity Project. 2005. *Main Report* (27 June). Archived at: <http://identityproject.lse.ac.uk/identityreport.pdf>.
- Martin, Aaron. 2012. National Identity Infrastructures: Lessons from the United Kingdom. In Magda David Hercheui, Diane Whitehouse, William McIver Jr. and Jackie Phahlamohlaka (eds) *ICT Critical Infrastructures and Society*. Heidelberg: Springer, pp. 44–55.
- Martin, Aaron and Edgar Whitley. 2013. Fixing Identity? Biometrics and the Tensions of Material Practices. *Media, Culture and Society* 35(1): 52–60.
- Martin, Aaron, van Brakel Rosamunde and Daniel Bernhard. 2009. Understanding Resistance to Digital Surveillance: Towards a Multi-disciplinary, Multi-actor Framework. *Surveillance and Society* 6(3): 213–232.
- Mathieson, S. 2011. Minister Destroys National Identity Register (10 February). Archived at: <http://central-government.governmentcomputing.com/news/2011/feb/10/minister-destroys-national-identity-register>.
- NO2ID. 2008. NIS Options Analysis Outcome. Archived at: [http://identityproject.lse.ac.uk/NIS\\_Options\\_Analysis\\_Outcome.pdf](http://identityproject.lse.ac.uk/NIS_Options_Analysis_Outcome.pdf).
- Otjacques, Benoît, Hitzelberger, Patrik and Feltz, Fernand. 2007. Interoperability of EGovernment Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems* 23(4): 29–52.
- Pieri, Elisa. 2009. ID Cards: A Snapshot of the Debate in the UK Press. *ESRC National Centre for e-Social Science* (23 April). Archived at: [www.ncess.ac.uk/Pieri\\_idcards\\_full\\_report.pdf](http://www.ncess.ac.uk/Pieri_idcards_full_report.pdf).
- Privacy International. 1997. History of ID Cards in the United Kingdom. Archived at: <https://www.privacyinternational.org/reports/history-of-id-cards-in-the-united-kingdom>.
- Sir James Crosby. 2008. Challenges and Opportunities in Identity Assurance (6 March). Archived at: [www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf](http://www.statewatch.org/news/2008/mar/uk-nat-identity-crosby-report.pdf).
- The Sunday Times*. 2006. Emails from Whitehall Officials in Charge of ID Cards. *The Sunday Times* (9 July). Archived at: [www.timesonline.co.uk/tol/news/uk/article684968.ece](http://www.timesonline.co.uk/tol/news/uk/article684968.ece). Now also available officially from [http://collections.europarchive.org/tna/20100429164701/http://ips.gov.uk/identity/downloads/foi/3905\\_URN\\_129.pdf](http://collections.europarchive.org/tna/20100429164701/http://ips.gov.uk/identity/downloads/foi/3905_URN_129.pdf).
- Torpey, John. 2000. *The Invention of the Passport: Surveillance, Citizenship and the State*. Cambridge: Cambridge University Press.
- UKIPS. 2006. Strategic Action Plan for the National Identity Scheme: Safe Guarding Your Identity (19 December). Archived at: <http://ips.gov.uk/identity/downloads/Strategic-Action-Plan.pdf>.
- UKIPS. 2007. National Identity Scheme Options Analysis – Outcome (leaked document), Identity and Passport Service. Available at: [http://identityproject.lse.ac.uk/NIS\\_Options\\_Analysis\\_Outcome.pdf](http://identityproject.lse.ac.uk/NIS_Options_Analysis_Outcome.pdf).
- UKIPS. 2008. Tracking Research. Archived at: [www.ips.gov.uk/identity/publications-research.asp](http://www.ips.gov.uk/identity/publications-research.asp).
- Warren, Adam and Elizabeth Mavroudi. 2011. Managing Surveillance? The Impact of Biometric Residence Permits on UK Migrants. *Journal of Ethnic and Migration Studies* 37(9): 1495–1511.
- Whitley, Edgar. 2009. Perceptions of Government Technology, Surveillance and Privacy: The UK Identity Cards Scheme. In Daniel Neyland and Benjamin Goold (eds) *New Directions in Privacy and Surveillance*, 133–156. Cullompton: Willan, pp. 133–156.



Proof

*Evolving identity policy in the United Kingdom* 219

- 1 Whitley, Edgar and Hosein, Gus. 2010a. *Global Challenges for Identity Policies*. Basing-  
2 stoke: Palgrave Macmillan.  
3 Whitley, Edgar and Hosein, Gus. 2010b. Global Identity Policies and Technology: Do  
4 We Understand the Question? *Global Policy* 1(2): 209–215.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

Taylor & Francis  
Not for distribution



24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45

Proof

