Journal of Southern African Studies, Volume 31, Number 2, June 2005

Routledge
Taylor & Francis Group

The Biometric State: The Promise and Peril of Digital Government in the New South Africa

KEITH BRECKENRIDGE
(University of KwaZulu-Natal)

In the political aftershocks of September 11, powerful interests in the United States and Britain have proposed the development of national systems of biometric identification and registration. For much of the last century, South Africans have lived with such a biometric order, and in recent years the democratic state has begun to invest in a massive scheme of digital biometrics for the delivery of benefits and the elimination of fraud. This HANIS system has been preceded by a massive project of digital biometric grant delivery that affects millions of people throughout the country. These systems are changing the nature of the state, and the relationship between private individuals and the commercial domain. For the countries considering a move from the decentralised order of paper-based identification to the new world of digital biometrics, there is much to be learned from a close study of contemporary South Africa.

Ten days after the events of 11 September 2001, Larry Ellison, CEO of the Oracle Corporation, gave a studio interview to a San Francisco television station. At the time Ellison was arguably the wealthiest man in the world, a celebrity billionaire, as flamboyant as Bill Gates is retiring. Since the mid-1970s his company has done more than any other to make networked relational databases a ubiquitous feature of modern government and commerce. Accordingly his thoughts on what Americans ought to do about the new dangers that surrounded them carried a certain weight. The remedy he suggested was one that is very familiar to South Africans: a fingerprint-authenticated identity document, and a national database to record the identity of citizens. Weeks later, in an interview with *Newsweek*, he backed away from the proposal for a national identity document arguing, instead, for what he called a biometric standard for drivers' licences, the most important form of personal identification. Citing the systematically integrated consumer credit databases as a model, he lamented the Byzantine archival structures of contemporary government information and called for the joining of commercial and government databases around a single biometric index. The key weapon in the effort to identify the new enemy within, he suggested, was a single national security database tracking these biometric identities. Using an infallible and unique index derived from each individual's distinctive biometric data, what computer scientists poetically call the superkey, this new national security database, as Ellison put it, will be 'the thing that really holds the truth'.[1]

In the months that followed, the ideas that Ellison had championed were given priority in the Bush administration's response to the crisis. The USA Patriot Act – passed in the shadow of the Attorney-General's warning that further attacks were imminent – added a host of new sources of financial and communications data, and legal mechanisms for officials to gather it

1 KPIX Eyewitness News at Five, 21 September 2001. 'A Techie's Solution', *Newsweek*, 29 October 2001, p. 64.

ISSN 0305-7070 print; 1465-3893 online/05/020267-16 © 2005 *Journal of Southern African Studies*
DOI: 10.1080/03057070500109458

secretly. Under the ham-fisted motto, *Scientia est Potentia,* John Poindexter's Office of Total Information Awareness (TIA) at the US Department of Defence's Advance Research Projects Agency began to lay out a massive project of government and commercial database integration in the search for the 'terrrorist's information signature'. The TIA also sought to encourage the deployment of new biometric tools like optical and facial scans to complement the use of fingerprint records as a binding link between the data and individuals.[2]

The clumsy dotcom enthusiasm of the individuals involved in the TIA made it spectacularly vulnerable to satirical critique, and the project lost ground from the onset. Not least as a result of Poindexter's own colourful history, his office attracted an enormous amount of political fire from both the left and the right. In the months after the 11 September attacks the project was in continuous retreat. First to go were the Masonic logo and the motto; then it suffered a name change from 'Total' to 'Terrorism' Information Awareness, to reassure law-abiding citizens.[3] Even Poindexter's resignation could not save the project from its congressional opponents. In September 2003 all funding to the TIA was eliminated, leaving the project's commercial and academic contractors high and dry. The demise of the TIA project, and the well-organised opposition to the idea of a national identification card in the United States, has done little to dampen the growing power of biometric technologies for personal identification, or the US federal government's interest in the use of a linked national security identity database.

Under the auspices of the Department of Homeland Security, the federal government is developing a national system of biometric identification by an ingenious process of reverse engineering. In both 2002 and 2003, the new Department of Homeland Security pursued the use of informational tools to secure the borders of the United States. Key to this effort was the introduction of biometric identification procedures at the ports of entry to the continental US. 'By October of this year', Secretary Ridge explained to CNN in January 2004, 'everybody coming across our borders is going to have to have a machine-readable passport with some other form of biometric identification'.[4] Biometric data from citizens from countries that require visas to visit the US (like South Africans) will be captured at the consulates in the home country and then confirmed upon entry to the US. Travellers from the European Union or Australia, who do not need visas, will be required to use passports that incorporate biometric identification systems.

This requirement of foreign visitors to the United States will impose a similar reciprocal identification procedure on Americans. Indeed the process is designed with that purpose in mind. Ridge explained recently that the US does not seek 'two standards' for international travel, and he has called on the European Union to work with the US in developing a single international standard for biometric identification. From October 2004 the United States was due to begin issuing an entirely new passport design, incorporating embedded smartcards that contain a public-key encrypted 'full-face image for use as a biometric'.[5] Using the new United Nations endorsed international standard, the passports will include other biometric indicators, such as digital fingerprints. Behind the airport terminals, a central database will retain 39 individual pieces of information about these travellers to the US for up to seven years after the visit.[6] The fact that the federal government has been able to use its immigration policy to hasten the global development of biometric identification technologies has not been

2 *Defense Week*, 23, 46 (18 November 2002).
3 The (once-extensive) TIA project has utterly disappeared from the DARPA web pages, but for a copy of the original see http://www.thememoryhole.org/policestate/iao/iao-original.htm
4 Available at http://www.cnn.com/2004/US/01/05/cnna.ridge/index.html (accessed 6 January 2004).
5 http://www.cnn.com/2004/US/01/05/fingerprint.program/index.html (accessed on 6 January 2004). http://www.theregister.co.uk/content/55/31885.html (accessed 5 January 2004).
6 http://www.tmcnet.com/usubmit/2003/Nov/1021112.htm (accessed 6 January 2004).

lost on its domestic opponents. 'Our government has forced on European governments the obligation to adopt biometric identifiers', the director of the Electronic Privacy Information Center noted recently, 'though most in the U.S. still oppose such systems'.[7]

Barely 2 per cent of Americans are issued with passports every year, so the arrival of what might reasonably be called a biometric order in the US seems distant. But there are many powerful forces moving the US informational infrastructure towards a single, biometrically authenticated and integrated system. The Association of Motor Vehicle Administrators has developed a standard for biometric identification technologies on drivers' licences which, although not mandated by law, has universal acceptance. Nor do individual Americans seem particularly concerned about leaving a biometric data trail. In June 2002, the largest grocery chain in the US, Kroger, ran a trial in College Station, Texas, that allowed customers to pay for their goods and earn loyalty discounts by using a registered digital fingerprint. In six months 10,000 of the 150,000 people who live in College Station had signed up to use the service.

There is no longer a plan for a national security database like the one originally developed by the TIA, but there is also already an extraordinary degree of database integration in the United States.[8] EPIC's Marc Rotenberg has aptly described the self-regulation of the commercial database industry as a '"race to the bottom" in which companies pursue ever more invasive collections of personal information'.[9] The Canadian, Australian and European legislative effort to bolster privacy in the face of the unregulated data-sharing of the 1980s and 1990s may have come too late. In 1999, Sun Microsystem's Scott McNealy pronounced that 'privacy is dead, get over it'.[10] Despite the passing of new federal laws that restrict the distribution of personal financial and medical data, the years since have seen the development of software and hardware that allow for the open-ended integration of commercial and bureaucratic data-sharing.

Larry Ellison's plan for a biometric identity card and a national security database has not come to life. But the United States and many other countries seem poised on the edge of embracing a fully-fledged biometric information order. This is a good time to consider how a biometrically organised society might function. Many questions about the social consequences of biometric technologies come to mind. Do they necessarily bring with them a certain kind of politics? Are they likely to improve the lives of individual citizens? Is a centralised system of identification, and regulation, compatible with the dispersed forms of bureaucracy that are currently in place in many of the western democracies? Will these tools necessarily harden the boundary between the prosperous societies of the West and the rest of the world? Will the private sphere dissolve under the harsh light of biometric data-gathering? And, finally, will these biometric systems actually work?

The rest of this article will show that South Africa is already a fully-fledged biometric order – a society characterised, on the one hand, by ubiquitous biometric identification and a centralised repository of this data, and, on the other hand, by a massive and unbridled commercial data analysis sector. Many societies, like Ivory Coast, have issued smartcard-equipped identity cards that also carry biometric data, usually in the form of digital fingerprints. But only a few have built a national database of biometric identities to authenticate and track the data carried and produced by the cards. Malaysia, Macao, Hong Kong and South Africa (all relatively prosperous societies adjacent to poor neighbours) are the first to implement such a system. South Africa is distinguishable from the others for two

---

7 http://www.nytimes.com/2003/08/24/national/24IDEN.html?th (accessed 24 August 2003). In Britain, the Blair government has invoked the US requirement to foster its own unpopular program for a biometric identity card, http://www.pcworld.com/news/article/0,aid,113846,00.asp (accessed 6 January 2004 at 3:34 pm).

8 S. Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol CA, O'Reilly, 2001).

9 http://www.epic.org/privacy/intl/EP_testimony_0200.html (accessed 7 January 2004).

10 http://www.wired.com/news/print/0,1294,17538,00.html (accessed 26 January 1999).

reasons. Like the United States, it has an extremely sophisticated and largely unregulated consumer credit industry.[11] In South Africa, as is likely to be the case in the United States, the two systems of data will mingle unhindered. And South Africa has a unique history of biometric control that underpinned colonial rule after 1900 as well as the system of apartheid. Biometric identification has been a ubiquitous feature of South African life for a century.

Unlike the Northern societies that now contemplate the introduction of biometric identification systems, South Africans have little choice about the development of biometric tools for personal identification. A century ago, Lord Alfred Milner fashioned a biometric regime around the collection and centralised processing of the fingerprints of African, Chinese and Indian people. These biometric controls were developed to overcome the failures of an existing system of documentary regulation, a system that I have called the archival state. Every generation since that time has witnessed an elaborate effort radically to overhaul the operations of the biometric identification regime in order to bolster the state's faulty grip on its subjects. Hendrik Verwoerd's *Dompas* system, which bears a striking resemblance to Larry Ellison's national security database, was the most radical of these schemes. The contemporary effort to build a new, fully digital national identification system is another.

In the US the effort to deploy biometrics today is a coercive project aimed at improving the state's surveillance. In contemporary South Africa this is also part of the state's interest in biometrics, directed particularly against immigrants and citizens who illegally claim welfare benefits. But it is also strongly motivated by a project of redistributive social justice. In contemporary South Africa the state's interest in digital biometrics is very largely driven by a desire to repair a broken bureaucracy, to deliver grants and other benefits to the poorest and most vulnerable of its citizens. There is a certain irony in the fact that these coercive technologies are now being applied to the task of hastening the distribution of benefits to those they were originally designed to subjugate.

Biometrics in the New South Africa

Combining the technologies of twenty-first century computers and nineteenth-century biometrics can produce startling results. Consider the South African Police Service's criminal records centre in downtown Pretoria. It is the physical qualities of this archive that are most immediately impressive. Two floors of the Sanlam Plaza in Schoeman Street are currently filled with metal cabinets of small, extendable drawers containing the fingerprints of 4.5 million convicted criminals. The oldest of these records date back to 1925. The physical weight of the collection is extraordinary – 15 years ago the records had to be moved because they threatened to bring down the building housing them.

The human characteristics of the centre are similarly remarkable. The archives are managed and searched by 100 'fingerprint experts'. Each of these people – many of them police detectives – has spent the better part of three years training to earn the legal capacity to present expert fingerprint evidence in a South African court. Between them they process an average of 3,500 fingerprint queries every day. Most of these requests for records are from the courts – from prosecutors looking to build cases against alleged criminals, and from judges and magistrates weighing up sentences. And the processing of requests is slow – moving the paperwork through the bureaucracy of the courts and police force takes 55 days, on average. The delay in the processing of fingerprints in order to establish criminal records is one of the reasons for the enormous number of awaiting trial prisoners in South Africa.

Early in 2002, the South African Police Service purchased an Automated Fingerprint Identification System (AFIS) from Sagem, a French biometrics company. The new system

11 Garfinkel, *Database Nation*, pp. 17–36.

involves the scanning of the entire paper-based collection into digital images, and the conversion of these images – without using Galton's lexical system of Loops, Arches and Whorls – into numbers. An individual fingerprint can be compared from a remote scanning point against the entire record set practically instantly. (Sagem have promised to reduce the amount of time taken to process fingerprints in the courts from two months to two days.) Computerised biometrics finally reduces the skills requirement to those, as Galton had naïvely claimed a century before, 'found in abundance among ordinary clerks'.[12] The two weeks of training required to operate the Sagem scanning equipment stands in outrageous contrast to the three years of experience required to read and accurately distinguish paper-based fingerprints with real proficiency. But most astonishing is the effect that the digitising of the fingerprint collection has on the physical qualities of the archive (and all that implies for the distribution and analysis of information). 'The whole library will be stored on two CDs,' the centre's Senior Superintendent Pine Pienaar observed, 'I still struggle to believe it'.[13]

There is also an old, familiar, imperative at work here. Like the laminated *Dompas* in the 1950s or the paper passports of the Milner period, the administrators implementing the new biometrics of our own era believe that they will radically improve the state's grasp of the identity, and history, of its elusive citizens. Along with the digital database of criminal fingerprints, the South African Police Service has invested in handheld mobile scanning machines capable of storing 50,000 fingerprints. These curiously named MorphoTouch terminals will access the central database using the country's ubiquitous cellular connections. Steve Tshwete, the recently deceased Minister of Safety and Security, announced that criminals will have 'nowhere to run'.[14] Computerised biometrics, like its paper-based predecessors, is driven by the fantasy of administrative panopticism – the urgent desire to complete and centralise the state's knowledge of its citizens.

Computers are particularly well suited to this task. Unlike punch-card readers which were purpose-built to process huge quantities of information gathered by people, computers started life as expensive calculators but soon found their purpose in tracking and analysing vast quantities of automatically generated 'feedback'.[15] In the military, in industry and in commerce, computers serve primarily as tools of automated surveillance, whether their subjects are radar signals, servomechanisms or nurses. Fifteen years ago, as the information technology era was just beginning to show itself, Shoshana Zuboff commented on the tremendous attraction managers feel towards the powers of the information panopticon. 'Information systems that translate, record and display human behaviour can provide the computer age version of universal transparency with a degree of illumination that would have exceeded even Bentham's most outlandish fantasies', she commented as the information technology era was just beginning to show itself. 'Such systems can become information panopticons that, freed from the constraints of space and time, do not depend upon the physical arrangement of buildings or the laborious record keeping of industrial information . . . [or] the presence of an observer.'[16] Zuboff's factory studies show that often the subjects of this panoptic power found ways to subvert the disciplinary intent of the systems of

12 F. Galton, *Fingerprints* (London, Macmillan, 1892), p. 15.
13 http://www.bday.co.za/bday/content/direct/1,3523,877969-6099-0,00.html (accessed 28 June 2001).
14 http://www.iol.co.za (accessed 20 March 2002).
15 On punch-card data-processors, see J. R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Harvard University Press, 1986), pp. 390–425, and E. Black, *IBM and the Holocaust: the Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation* (London, Little, Brown and Company, 2001). On the early computers and the processing of electronic feedback, see D. Noble, *Forces of Production: A Social History of Industrial Automation* (Oxford, Oxford University Press, 1984), pp. 42–76, and P. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MIT Press, 1996), pp. 43–111.
16 S. Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York, Basic Books, 1988), p. 322.

Figure 1. MorphoTouch Fingerprint Identification Terminal.[17]

automated surveillance, but she also documents an overwhelming bias toward automated surveillance. It is the attraction of an automated, and apparently infallible, 'informated' state that lies behind the renewed interest in biometrics in South Africa (Figure 1).

This process of establishing the biometric state is still in its early phases but is also clearly irreversible. The rest of this article will chart some of the ways in which biometrics is changing the state's practice, and pose some questions about the implications all of this has for our understanding of bureaucracy and individual identity.

Biometric Pensions in Zululand

The earliest forms of computerised biometrics in South Africa were deployed in the effort to regulate the movement and work of labourers on the South African gold mines.[18] The technology has moved very quickly beyond the world of industrial work. The first large-scale application of fingerprint-based digital biometrics was in the delivery of pension benefits in the former KwaZulu homeland in 1990. Faced with the task of providing pensions to rural areas without anything resembling infrastructure and no banking facilities of any kind, the KwaZulu government accepted a tender from a joint venture of First National Bank and an IT firm called Datakor – the locally owned remainder of the disinvested Unisys Corp. The new company was called Cash Payment Services (CPS), and it organised the distribution of pensions using biometric identification that was, to say the least, internationally precocious. (In 1996, CPS won the Computerworld Smithsonian Institution's financial services innovation award for its biometric identification software.) By the middle of the 1990s, CPS was using four-wheel drive vehicles to dispense pensions in the KwaZulu and Kangwane homelands to some 400,000 individuals. The system involved the prior digital registration of fingerprints which were then stored on a card bearing a magnetic strip and on a central database. Pensioners received their cash from the truck-mounted dispenser after pressing their forefinger onto a CPS scanner attached to a computer.[19]

CPS presented a compelling remedy to the provincial states' administrative and infrastructural incapacity, especially in the risky distribution of cash pension payments in the countryside. By the end of the 1990s, they were providing pensions and unemployment benefits to over a million people from some 5,000 fixed and mobile sites in six South African provinces and neighbouring Namibia. In KwaZulu-Natal the company equipped post offices with its fingerprint scanners to channel payments to pensioners in the towns and cities.

17 http://www.sagem.com/en/produits-en/biometrie-en/terminaux-biometriques-en.htm (accessed 1 October 2002).
18 See J. Crush, 'Power and Surveillance on the South African Gold Mines', *Journal of Southern African Studies*, 18, 4 (1992).
19 *Financial Times* (London), 16 February 1996, p. 4.

The original CPS system had made use of single-purpose magnetic-strip cards to store biometric identifiers, but towards the end of the decade the cards began to change.[20]

In 1999, CPS was purchased from First National Bank by Aplitec, an innovative South African IT company specialising in the development and manufacture of smartcards.[21] From this point, the fingerprint pension distribution scheme became harnessed to a much more powerful multi-functional smartcard. These new cards became the vehicle for the pension payments – instead of a direct cash payment after presenting their fingerprints, pensioners now receive a credit directly onto their Aplitec smartcard, which can then be used immediately to draw cash from an adjacent cash dispenser. But the cards were only secondarily identification tools – they were intended primarily to make the otherwise utterly secluded cash economy of the rural pensioners 'bankable'.[22]

The smartcards were designed to provide a host of new services. In 1999 the company entered into an agreement with the South African Local and Long Distance Taxi and Bus Organisation (SALLDTBO) to install smartcard readers on 20,000 taxis operating from the organisation's 200 ranks. By the end of that year they had installed readers on about 2,000 taxis, but the taxi installations have not been a success. The smartcard was also originally intended to displace the use of cash altogether in the payment of retail goods, pre-paid electricity, water and telephone bills and even healthcare. This effort to reorganise the cash economy around the Aplitec smartcard seems, to date at least, to have failed.

It has been primarily in the area of financial services that the smartcards have wrought the most significant changes. Aplitec immediately began to make the smartcard's automatic deduction facilities available to a small group of companies providing services like family funeral policies and life assurance. A company called Cornerstone, for example, provides life assurance policies to some 230,000 pensioners in KwaZulu-Natal and Mpumalanga, using the risk-free deduction facilities provided by the smartcards. More recently Aplitec has begun to offer short-term credit facilities directly to grant-holders. The Black Sash has recently complained to the minister that this system of automated deductions, which leaves the most important choices of service provider and payment in the hands of Aplitec, places pensioners at a financial disadvantage. The provision of short-term credit to grant-holders is undeniably an invaluable service, but the massively decreased risk that Aplitec faces in the provision of these loans – unlike all other short-term credit providers, Aplitec's investors are guaranteed regular repayments – ought to result, as the Black Sash has suggested, in discounts to the recipients.[23]

The company's hold on the distribution of pensions in South Africa continues to strengthen. In February 2002, Aplitec was awarded part of the Eastern Cape's pension grant distribution, giving them control of more than 70 per cent of the welfare and social grant system in South Africa. At the start of 2004, some 2.5 million recipients used Aplitec's biometric 'citizen card' at 7,500 payout points to receive state pension and child support grants.[24] Smaller smartcard welfare schemes have been designed and implemented by Aplitec in six other African countries. At a time when most other IT companies have been hiding from their shareholders, this one has been paying dividends. Aplitec was the only IT company on the Johannesburg stock market whose share price increased during the three years that followed the collapse of the global IT bubble after March 2000 (Figure 2).

---

20 http://www.aplitec.co.za/aplitec/cs/brochure_pension1.htm (accessed 1 October 2002).

21 Net1 Aplitec was responsible for the switching infrastructure for the SASWITCH automated teller machine network that was developed in 1987.

22 http://www.aplitec.co.za/aplitec/aplitec_aquisition.htm (accessed 26 March 1999).

23 http://www.cornerstonegroup.co.za/background.htm (accessed 1 October 2002); http://www.blacksash.org.za/display.asp?article = 14 (accessed 11 April 2002).

24 http://www.itweb.co.za/sections/business/2003/0306051226.asp?A = FIN&S = Financial&T = Financial&O = L (accessed 4 January 2003).

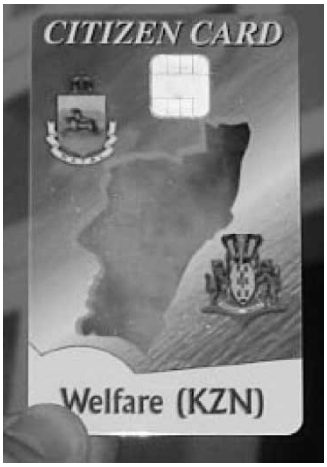

Figure 2. Aplitec's KwaZulu-Natal Citizen Card.

Issuing grants to enormous numbers of people has been handled with remarkable efficiency under the Aplitec contract, but it has not been completely free of problems. Pensioners generally arrive very early – often before dawn – on their assigned day of payment, and they often have to wait for hours before receiving service. In mid-2003, several grant-holders in the Eastern Cape died while waiting for payment, and others complained bitterly of having to wait for hours for CPS trucks to arrive. Amidst a chorus of anger from the most underdeveloped region of South Africa, Minister of Welfare, Zola Skweyiya, denounced the CPS contract. Accusing the company of 'gross and flagrant violations' of the terms of the contract and the 'human and constitutional rights of our people', he called for an end to the contract.[25] In a characteristically frank statement, Aplitec defended its performance in the Eastern Cape, its rights under the contract, and revealed the sorry state of government electronic record keeping in the region.[26] A very public disagreement between the Eastern Cape government and the company was concluded by the government reverting to the payment of pensions by hand in six of the least organised districts. Aside from the appalling state of government records in the former homelands, the conflict highlighted a new kind of politics between elected officials and the private companies that increasingly handle many of the core activities of the state. Elected national and provincial officials are vocal in the effort to ensure reasonable service from the private companies employed to handle tasks – like grant delivery – that the state has to date been unable to perform. And the companies, like CPS, have only a limited ability to accommodate these demands, given their essential interest in securing a profit from government contracts.

Even the normal operations of this biometric system highlight some of the boundaries of computerised biometric technologies. The mobile payout points and the fingerprint scanners that CPS uses have been carefully 'ruggedised' to help them withstand the battering handed out by rural roads, but unfortunately the fingers captured by finger-printing tend not to be very reliable in the long run. The technicians who capture each individual for the CPS database carefully record ten fingerprints. The best four of these prints are recorded on the Citizen Card, and for good reason. Even a simple cut can make a finger unreadable, and it is quite

25 http://www.dispatch.co.za/2003/06/12/easterncape/AAAALEAD.htm (accessed 12 June 2003).
26 http://www.theherald.co.za/herald/2003/07/04/news/n20_04072003, and http://www.aplitec.co.za/Pressreleases/Aplitec_04_07_2003.htm (both accessed 4 July 2003).

Figure 3. Scanning Fingerprints at Umlazi Paypoint.

common for grant-holders to actually lose the finger that was originally chosen to secure the payment card. The prospect of thousands of individuals mangling their fingers to avoid being picked up by police fingerprint scanners begins to seem less ridiculous after a visit to one of the payout points. Much more remarkable, given the prevalence of subsistence crime in South Africa, is that technicians who are responsible for delivery of these biometric systems in KwaZulu-Natal have never witnessed an attempt at biometric impersonation – in other words, they cannot remember a single instance of an individual attempting to draw cash from a payout point using someone else's citizen card. This is quite remarkable testimony to the disciplinary success of CPS's biometric pension scheme (Figure 3).

Yet, in another crucial respect, the company has been a victim of its own success. In the last year, Aplitec has been busily extending the micro-lending services it offers to its pensioner clients 'in order to ensure their long-term loyalty and support' in the face of an overwhelming competitor – the national government.[27] The former Chief Minister of KwaZulu and current national minister of Home Affairs, Mangosutho Buthelezi, was obviously much impressed by the fingerprint-identified pensions scheme he first implemented in 1990, and he has resolved that a similar scheme will serve as the basis of a new national identity document. This system has been designed to mimic all the identification and financial functions of the Aplitec smartcard but on an even grander social scale.[28]

HANIS is the Answer!

The current South African Department of Home Affairs (DHA) has inherited a set of formidable problems from the apartheid state. One of the most difficult of these is the maintenance of the

27 http://www.aplitec.co.za/aplitec/Annual_report_2001/1ceo_statement.htm (accessed 30 June 2001).
28 http://m1.mny.co.za/BBStks.nsf/Current/C2256A2A0053166642256C17001AFCAA? OpenDocument (accessed 16 August 2002).

national Population Register. This database is the lynchpin of official identity, life, death, marriage and citizenship in modern South Africa. It was also, as Deborah Posel has shown, the administrative and ideological cornerstone of apartheid, and it reflects the particularly demented data-gathering obsessions of that era.[29] The official racial identity of White, Indian and Coloured citizens of South Africa was established and recorded in one database by the Census Bureau after the passing of the 1950 Population Registration Act. Africans were recorded in a separate Population Register developed and maintained by the Central Reference Bureau in the process of issuing *Dompas* identity books to men and women after 1954. This register, and particularly the fingerprint classification effort, was in complete disarray by the early 1960s when another set of even more dishevelled databases was added to the mix.

As the homelands of Transkei, Bophutatswana, Venda and Ciskei began to adopt the Verwoerdian programme of national independence, they took responsibility for recording the identity, births, marriages and deaths of their putative citizens. The opportunities for duplication and error began to accelerate as the remaining African reserve territories wobbled into an administrative status that was labelled 'self-government', and took on their own population registers. By the end of the apartheid period over a dozen discrete yet overlapping and duplicated population registers were in place. To this mess was added, in February 1991, a newly deracialised national population register that dissolved the old racial databases but did not incorporate the 'independent' homelands. These records were returned to the national register in 1994, at the formal birth of the new South Africa. The combined register has inherited the data structure and content of all of these previous databases and is only as reliable as the original data collection of each of those.[30]

As a direct inheritance from Verwoerd's *Dompas*, the only mechanism for ensuring the integrity of the data is a single enormous collection of fingerprints. To date the Home Affairs fingerprint collection numbers some 40 million sets, which is ten times the size of the almost unmanageable collection maintained by the South African Police Services. Fingerprints were collected on the issuing of all identity documents – either originals or duplicates, and they are taken from all legally contracted foreign workers and all repatriated illegal immigrants. Every day the collection increased by some 7,000 prints. 'The nagging tedium that comes with the duty to manually and physically reach and scrutinise the fingerprint records becomes', as an official Home Affairs statement put it, 'nightmarish to contemplate'.[31] Considering the opportunities and incentives for dissembling, impersonation and duplication under apartheid, it seems clear that the register was broken.

For the officials in the DFA – charged with maintaining the integrity of the documents of individual identity – the 'leaky' population register is the single cause of a host of problems – fraud and corruption in the distribution of social benefits, massive illegal immigration and unchecked crime. It was for this reason that the new department moved very quickly to secure interdepartmental and cabinet approval for a mechanism for repairing the Population Register and issuing new identity documents. 'HANIS, the Home Affairs National Identification System is the ultimate brainchild of the struggle against crime caused by the susceptible identification system here', an official account explains. 'The Department exudes confidence that this is the answer!'[32] And Home Affairs seems to have been joined in this enthusiasm by the other departments and their ministers. By January 1996, very early on in the slow-moving policy-making agenda of the new democratic state, the national cabinet had agreed to the new

29 D. Posel, 'Race as Common Sense: Racial Classification in Twentieth-Century South Africa', *African Studies Review*, 44, 2 (September 2001), pp. 87–113.

30 http://www.dpsa.gov.za/SDILearningNetworks/LrngNtwksdocuments/E-gov/HANIS-PresentationOct01.pdf (accessed 1 October 2000).

31 http://home-affairs.pwv.gov.za/projects.asp#project2 (accessed 1 October 2002).

32 http://home-affairs.pwv.gov.za/projects.asp#project2 (accessed 1 October 2002).

system, and the process of establishing a national biometric identification register began, very slowly, to come to life.

The project has changed a lot over the last five years, but the original tender – estimated to cost around R600 million – consisted of three parts: the creation of an automated fingerprint system, integration of this system with the current population register, and the establishment of a card-issuing facility. The tender was issued in December 1996, but only awarded some two-and-a-half years later. Along the way some of the most powerful international contractors in the field – including Lockheed Martin, the company responsible for digitising the FBI's database of 40 million fingerprints – were eliminated. After an investigation of the tendering process by the public protector, the contract was eventually awarded to a consortium headed by a company, dubbed Marpless, made up of the union of Japanese conglomerate Marubeni, Inc., and Plessey, itself jointly owned by Dimension Data and Worldwide Africa Investment Holdings. In the intervening period as the requirements of the department and the technology altered so did the contract.

The original model for HANIS in 1996 was very close in form and function to the system of pensions delivery being used by CPS in the KwaZulu countryside. It required a fingerprint database, a software system and infrastructure for delivering services, and a set of magnetic-strip smartcards for identifications. By 1999, the cabinet was determined that the contract be adjusted to make use of smartcards and their enhanced security and applications. The company that had been selected to provide the magnetic-strip cards – Polaroid – was not in a position to meet these new demands, and they withdrew from the tender. The reaction to the Department's request for proposals for a new and separate smartcard tender suggests that there are several local and international candidates very keen on providing them. But there is currently no consensus on the range of functions to be included on the cards, no contractor selected, nor is there any meaningful estimate of the total cost of their production, although the figure of R3 billion is widely discussed in the press.

The problem of the population register required similar adjustments. The tender had called for an Automated Fingerprint Identification System (AFIS) without much in the way of specification. Towards the end of 1999, Marpless was awarded an R800 million supply contract with Home Affairs to produce the AFIS. The Japanese firm NEC produced the hardware and scanning technology and Unisys was responsible for integrating all the different systems (including the as yet unspecified smartcards and the population register). The AFIS computer systems – installed in the appropriately named New Co-operation Building in central Pretoria[33] – began working in February 2002. The key tasks of converting the collection of current records and then extending it to the local branches of Home Affairs have only just been initiated.[34] But the officials are optimistic. 'HANIS,' Minister Buthelezi declared at the commissioning of the basic system, 'is a clear example of how South Africa can leap-frog ahead and set the basis to redress our grave and many shortcomings by implementing solutions which are ahead of the times'.[35]

A Single View of the Customer

The substance of the new HANIS identity system will not be determined by the digital population register, nor by the software and networking tools that connect the different scanning interfaces together. The informational order of post-apartheid South Africa will be

33 http://www.dpsa.gov.za/e-gov/2002docs/newsletterMay2002.pdf (accessed in May 2002).
34 http://www.pmg.org.za/overview/update/home.htm (accessed 1 October 2002); http://www.pmg.org.za/docs/2002/comreports/020606pchomereport.htm (accessed 4 June 2002).
35 http://www.queensu.ca/samp/migdocs/speeches/180202.htm (accessed 1 October 2002).

made by the range of applications that the chips on the cards support. These have not yet been decided – primarily because the list of applications is already extremely wide-ranging. For most of 2004 a HANIS Interdepartmental Technical Committee was designing a standards-based system that will allow the many different government departments and commercial interests to make use of the cards. The plans for these cards are little short of astonishing.

When Billy Masetlha, the Director-General of Home Affairs, convened an Interdepartmental Workshop on Biometric standards, his presentation left little doubt that the cards will be designed to interact seamlessly with at least three new large-scale data-sharing systems. The first and most advanced of these is the South African Police Service's newly automated criminal records database. These records, in turn, have been designed to interact with another complex data and process sharing arrangement between the courts (Justice), the prisons (Correctional Services) and social welfare officers (Social Development). One part of this new data handling arrangement is called the Court Process Project, and it is a networked and digital document handling system designed 'to integrate their processes and pass information and data electronically to each other in order to improve administration and handling of dockets and case files'.[36] The Department of Transport similarly requires the use of the biometric identifier to authenticate drivers' licences and, presumably, to implement a national system of penalties. And, finally, the Department of Social Development will use the cards to authenticate payments to welfare grant beneficiaries and, in all likelihood, transfer funds directly. In short, the smartcards are to be the lynchpin of a transformed and networked state. They are being designed to interact with all the major sources of government information about its citizens, and most importantly, to offer the state a panoptic 'single view of the customer'.[37]

Nor are the applications on the smart identity cards to be restricted to government functions. In launching the new AFIS system, Minister Buthelezi indicated that the state has every intention of encouraging businesses to develop applications for the cards. 'By itself this system will make the smartcard a great contribution to the development of private sector initiatives', he remarked in February 2002, 'it can be used for identification purposes in building access control or by vending machines which intend to restrict their products, such as cigarettes, to adults only'.[38] When Home Affairs issued a Request for Information (RFI) about the design of the cards, they received – to their astonishment – over 60 responses from local and international businesses. By that stage it was quite clear that, as one of the local computer magazines observed, 'HANIS is IT on the scale of Grand Opera'.[39]

From April 2002 three working groups representing business and government interests were convened to discuss the most important issues. The first group was formed to examine the technical standards for the card, the capacities of the chip it will carry, and the problem of card security. Another group will consider the other smartcard projects – such as Aplitec's pensions system – already underway in South Africa. And the last group, consisting primarily of the South African Banks and the consortium of Europay, Mastercard and Visa (EMV), will look at the ways in which the cards can be made to interact with the banks' existing infrastructure, current international standards for smartcards and the new 'electronic purse specifications'. A more full-bloodedly commercial design process is hard to imagine.

Nevertheless, there is almost no official and very little public concern for individual privacy, the probability of data-creep on a large scale, and almost open-ended possibilities for abuse. The minister has, on several occasions, indicated the need for restraint and

---

36 Department of Home Affairs. 'Position paper with regard to the establishment of a national fingerprint biometric standard for government', VERSION 1.0 NOVEMBER 2001 http://home-affairs.pwv.gov.za/documents/presentations/position%20paper.zip

37 http://home-affairs.pwv.gov.za/news.asp?id = 2 (accessed 1 October 2002).

38 http://www.itweb.co.za (accessed 19 February 2002).

39 http://www.computerweek.co.za/pebble.asp?relid = 16045 (accessed 31 March 2002).

the necessity to restrict the applications served by the smartcards. But his most recent statements – and the planning of the department – reflect little of this caution. The political implications of the new identification system form one, minor, part of a commission set up under Fink Haysom to monitor the entire tender process.

Comparisons

Given the history of identity documents in South Africa, it would be foolish to attempt to evaluate the implications of the HANIS system before a single smartcard has been printed. One point is fairly clear, however. South Africa is going to be one of the first countries to implement a biometric national identifier. The DFA delights in this fact: 'In terms of the system magnitude, we are the pioneers.'[40] But why is it that South Africans are implementing computerised biometric registration so early? And why have other societies chosen not to do this?

Only a few other societies use smartcards as national identification documents. In Europe, according to the Gartner Group, only Finland has issued smartcards in anything approaching significant numbers, and their design is very unlike the ones intended for use in South Africa. Like HANIS, these cards are linked to a national population register, but they work using the very extensive Public Key Infrastructure supported by the Finnish cellular network providers. The smartcards carry a digital certificate using a private key registered for each citizen by the national population register. Like the cellular system in operation in South Africa at the moment, this private key system will be harnessed to a set of smartcard readers provided by the Ericsson subsidiary, iD2. Connected to computer desktops or PDAs, these card-readers will allow Finnish citizens 'to officially register a change of address, access day-care, library and banking services and even reserve a tennis court at the local sports centre – anytime of the day and from any location that offers Internet access'.[41] The Finnish smartcards are intended primarily for online use, they will have no biometric identifier, and they will not carry applications for government ministries and the commercial banks.

Towards the beginning of 2001, the Chinese government announced the development of a new national identification document very much like the system being developed in South Africa. This new card is also intended primarily to serve as an identity document and an authenticating tool for social welfare. It will also include a microchip that will contain an as yet undecided list of official records. 'This invisible information will include the same printed details [as appear on the card], plus fingerprint biometric data for identity validation', Gartner relates. 'It may also contain a driver's licence, a passport, financial details, insurance coverage, welfare benefits and criminal records.'[42]

There are several key differences between the two projects, however, not least the informational legacy of apartheid itself. The South African smartcard forms part of an effort to repair already existing databases in the Population Register and the SAPS Criminal Records Centre (and their associated fingerprint registries). It is intended as a digital extension of these existing biometric systems. The second major difference is that, without commercial banks, there is no meaningful credit infrastructure in China, and none of the risk evaluating databases associated with this kind of credit management. In South Africa, the smartcard will be implemented amidst an extremely sophisticated banking data-handling environment. The South African smartcard will begin its life saturated by data-gathering sponsored by both the state and business. And, finally, there is the question of scale. The Chinese project will be delivered to a billion people, many of whom live a great deal further

40 http://home-affairs.pwv.gov.za/projects.asp#project2 (accessed 1 October 2002).
41 http://www.id2tech.com/presscorner/docs/990712.htm (accessed 12 July 1999).
42 http://www.gartner.com COM-15-4370 (accessed 19 February 2002).

from a meaningful technology infrastructure than is the case in South Africa. The time required to implement the system is currently estimated to be at least a decade, at which point the cards will probably require reissuing. Given the smartcard infrastructure that is already in place, the South African project is likely to be much more rapidly achieved. In short, while the Chinese project shares many informational and administrative objectives with HANIS, the South African project is likely to produce the first genuinely digital biometric society.[43]

Why Are We Alone Out Here?

Why is it that none of the other industrialised capitalist societies have a similar scheme in place? In the months immediately after the events of September 11, Gartner's research showed that smartcard identity documents were not officially being planned in Germany, France, Britain, Denmark or Sweden. In the years that have followed, an intense debate about the place of biometric identification has erupted in Europe, and particularly in Britain under the influence of the recently unseated Home Secretay, David Blunkett. Yet, in many of the European countries there are very strong political and constitutional imperatives that limit the use of a single national identification number. And the possibility of the kind of open-ended data-sharing envisaged for HANIS is simply inconceivable in most of Europe, where powerful data-integrity laws already exist. With the forthcoming immigration and social services integration in the European Union there is every likelihood that the localised and contingent documents of identification will remain dominant within Europe for the foreseeable future.[44]

And what of the United States? The debate about a national identity card, national security database or a single driver's licence system to replace the current localised identity system continues. Until recently, almost all official identification has been handled by local vehicle licensing departments. These systems are not nationally integrated or compulsory. Increasingly it appears that the federal government will impose a biometric system without actually legislating. But what is striking in this debate is that the most influential information technology research company, the Gartner Group, has come out in opposition to biometric identity documents. This is particularly interesting as many of Gartner's largest clients (like Larry Ellison's Oracle Corporation and Scott McNealy's Sun Microsystems) would be likely to benefit from the enormous direct and indirect spending on hardware and software that would result from the deployment of a national biometric identity system. Gartner's reasoning for not implementing smartcard identity systems is compelling, and it raises the prospect of four sobering problems for the deployment of a biometric population register like HANIS.

The first serious problem with the implementation of a digital biometric identity document is likely to be the problem of deliberate or accidentally mistaken identity. The biometric data contained on a smartcard and on the national database is only as reliable as the original scanning – whether manual or automated – and only as secure as the trustworthiness of the officials charged with this task. The possibilities for error and fraud in the already existing database are very significant. In a population of tens of millions there will certainly be some real and accidental matches. What will happen to the citizens whose identity is contradicted, or deliberately stolen, using the biometric data housed in the databases? The authority of networked computers is already difficult to contradict – the added power of unmediated digital scanning is surely likely to increase this risk.

---

43 The Hong Kong government has begun implementation of a very similar biometric smartcard system called the Smart Identity Card System (SMARTICS). While the Hong Kong system includes many of the data and privacy concerns of HANIS, it is not a national system and it is designed to control migration between the city and its rural hinterland. Much of the real significance of the South African system will be in its implementation in the rural reserve territories. See http://www.gartner.com COM-15-4907 (accessed 15 February 2002).

44 www.gartner.com SPA-15-4207 (accessed 21 February 2002).

A second and related concern is the problem of security. There has been much discussion about the technical specification for the HANIS databases and the cards. But strikingly little of this has been about how the networked databases, and the cards themselves, are to be protected from illegal access. Referring to the United States, Gartner makes the chilling point that 'there is no reason to believe that governments or the private sector can provide affordable data repositories that are immune to attack using current computer and network technology'. This is especially the case because the South African computer systems are positioned on a global network, and they are likely, indeed certain, to be targets of the most sophisticated hacking efforts once the HANIS system is in place. The illegal financial rewards for successfully hacking a national identity repository would be very great indeed. Nor is the Internet the only problem here – the opportunities for internal official misuse of the highly portable data are almost infinite.

There is also the problem of the future. The cryptographic systems deployed on the cards today are very unlikely to be worth very much in a decade. In short, 'biometric data cannot be adequately protected on cards that may be used for five to seven years'. The biometric state – South African, American or British – is very likely to find itself defending, once again, a massive documentary battlefield (of its own making) in the effort to defeat relatively small numbers of well-organised insurgents.

Finally, there is the problem of 'data-creep'. In many respects the South African cards are being designed to allow data indexed on the fingerprints to flow from one contiguous database to another. The voluntary provisions (presumably modelled on the Online Protection Alliance) of Chapter VII of the Electronic Communications and Transactions Act of 2002 will not serve to halt the likely commercialisation of transaction data that will follow from the widespread use of the cards for identification and payment. What is to prevent the company that owns the networked cigarette vending machines, discussed by Minister Buthelezi on the commissioning of the HANIS system, from selling the data (including the product, amount and time of purchase) about the individuals who use them to employers or marketers? This cross-referenced data gathering is antithetical to almost any idea of privacy – and certainly runs against the privacy rights enshrined in the South African constitution. It is principally for this reason that most European democracies have chosen not to implement a biometric system.

To this list of Gartner cautions, South Africa's experience of digital biometrics should add another. The combination of digital scanning and networked information radically alters the characteristics of bureaucratic forms, removing them from the world of paper-based documents, and – more importantly – from the domain of human agency. The best new forms of biometric identification are very fast, very accurate and, as the CIA's John Woodward advises, have 'no human decision-maker in the decision loop'.[45] The economic and administrative benefits that follow from this removal of the 'human decision-maker' are ineluctably moving the South African state towards networked and computerised biometrics as the core practice of the state. Yet, as the CPS debacle in the Eastern Cape, and the massive chaos that has followed the similarly organised credit card driver's licence scheme have both shown, centralised databases are very blunt instruments, particularly badly suited to the task of repairing errors that are produced on the ground. This is because 'data-driven' government usually (not necessarily) disempowers local officials, who have limited rights to edit records, or change the rules embedded in the database. Implicit in the removal of the bureaucratic interpreter is the removal of all other kinds of subject-determined identity.

These biometric technologies may resolve some of the gaps and anomalies in official information about individual citizens, but they may do so at the cost of individual citizens' control over their own identities and the bureaucracy's capacity to mediate. The real likelihood here is

45 http://www.sjsu.edu/faculty/kpnuger/Privacyweb/Biometrics.htm (accessed 1 October 1997).

that the huge investment in centralised information systems will not be matched by a similar investment in the training and human resource capability of key elements of the state bureaucracy. The results of what we can describe as the state's normalising project – the most important contemporary examples include interventions to remedy or prevent child abuse, violence against women or the elderly – are likely to be very damaging in the long run.

Conclusion: An Archival Legacy

In South Africa there is no meaningful alternative to the HANIS scheme. The informational predicament in which South Africans find themselves is a product of a long history. The move from archival to database government began in the 1950s. There is no exit point. The African National Congress and its government partners cannot, as the revolutionaries did in France in the 1780s, simply destroy the records of the *ancien régime.* But we can certainly do more to limit the damage that this new system may yet produce. Key here is to establish concrete limits, and penalties, on the exchange of data for commercial gain, especially those that relate to individual and household privacy. An explicit legal understanding of the nature, and rights of the private sphere, would do a great deal to limit the otherwise unconstrained rationalisation of privacy that will follow from the widespread use of a biometric identifier.

A second, related project is to begin to chart what a confessional datasphere might look like: what kinds of information ought to be protected by statute? Examples might include mundane data trails like video and book rentals and subscriptions, or more rousing characteristics like medical records, religious affiliation, or racial, ethnic and linguistic inheritance. In each case, the data associated with each of these characteristics may be used to limit or remove the rights that individuals currently enjoy, and it would require only a very short historical excursion to explain how. Unfortunately, there is currently no sign of a legislative or popular effort to slow down what Habermas has described as the system's colonisation of the lifeworld.[46]

A final point about the South African project is that a notion persists in government, the media and the academy that information technologies affect only the lives of the wealthy, connected bourgeoisie. In that argument, digital tools affect the poor, who live beyond the 'digital divide', only by stripping them of jobs. The CPS pension system, HANIS and other massive schemes like the Department of Transport's Taxi Recapitalisation and Credit Card Licensing schemes, contradict this idea utterly. The very poor – the so-called 'poorest of the poor' – are in direct contact with these cutting-edge technologies and the database systems that maintain them. Indeed, information technologies have affected them much more powerfully than their middle-class contemporaries.

What then of Larry Ellison's proposal, and the questions prompted by the debate around the making of a biometric state? If there is a single lesson for countries like the US and Britain, contemplating a shift from the disorderly documentary world of archival government to the bright new world of the biometric database, it must surely be that biometric government has not, historically or presently, worked very well in South Africa. It shows few signs of being able to repair itself, but cannot easily be reversed.

Keith Breckenridge
Department of History, University of KwaZulu-Natal, Durban, 4041, South Africa. E-mail: breckenr@ukzn.ac.za

46 J. Habermas, *The Theory of Communicative Action, Volume 2: Lifeworld and System: A Critique of Functionalist Reason*, Translated by T. McCarthy (Boston MA, Beacon Press, 1987), pp. 153–96.