



Biometrics: the future at our fingertips?

Event Report by Dr Henry Kippin

*The **Social Market Foundation** is an independent public policy think-tank, developing and advancing innovative solutions across a broad range of economic and social policy. We publish original research, hold seminars and debates in Westminster and beyond, and run a diverse programme of events at the three main party conferences. Since its foundation in 1989, the work of the SMF has been principally devoted to promoting the social market philosophy, which seeks to marry markets and social justice. It neither sees the market as a necessary evil nor as an end in itself but as a means to improve people's lives. It is underpinned by adherence to two key principles: first, a positive preference for market mechanisms, while recognising that a truly pro-market approach is often not a free-market one; and second, a belief that a sustainable market economy rests on social and political foundations that are widely regarded as fair. Our work aims to elucidate these ideas and to explain why the social market is a fruitful source of solutions to public policy problems.*

Social Market Foundation

11 Tufton Street
Westminster
London
SW1P 3QB
phone 020 7222 7060
info@smf.co.uk
www.smf.co.uk



Biometrics: the future at our fingertips?

Biometrics are at the centre of some of the most heated ongoing debates in British public life. Often the term is caught up within highly polarised arguments around ID cards, public surveillance and counter terrorism measures. It is clear, however, that there is a separate debate to be had around the practical implications of the ever-increasing utilisation of biometric technology in everyday life, which is often overtaken by these other discussions.

Arguments over security versus liberty have most recently come to the fore in reaction to the Omand report, which advocates a more expansive sharing of personal data (including biometric data) across those public bodies responsible for maintaining national security. 'Access to such information' it is argued, 'might well be the key to effective pre-emption in future terrorist cases'¹. The intrusion into individual privacy this would necessitate is, however, too high a price to pay for some. The Convention on Modern Liberty – a recently formed pressure group – has argued that Britain is already subject to a 'silent but deadly accumulation of police powers'.² For them, the collection of biometric data represents the top of a slippery slope that leads to the inevitable erosion of civil liberties and the beginnings of a 'surveillance state'.

Elements of this debate have already been played out at the Social Market Foundation, which hosted a keynote speech by Home Secretary Jacqui Smith in November 2008. In it, she argued that the use of biometric data in national ID cards was essential in addressing a growing need for us to prove our identity – 'subject to common standards, and common standards of the highest security'.³ In order to achieve this, the Home Secretary has argued that basic personal information on ID cards would need to be enhanced by microchip technology linking to a biometric database of fingerprints.⁴

Whilst these debates rage on around it, the biometrics industry appears in good health. According to a recent *Daily Telegraph* report, the UK market alone is 'worth £311m a year'. Globally, an industry already thought to be worth £1.2bn is expected to grow to almost £5bn by 2012.⁵ Why? One obvious trigger was the events of September 11th 2001, after which point the use of biometrics in the security industry mushroomed from being a 'marginal player in the...field'⁶ to an industry of central importance. This trend has impacted on the areas one might expect – on airport security and national identity schemes for instance – but also on other commercial and public policy environments. In the U.S., biometrics have been used to combat benefit fraud; meanwhile the casino industry has employed facial analysis technology to 'create a facial database of scam artists'⁷. Most recently, the UK's Olympic Delivery Authority has announced the use of 'face and palm recognition techniques' on the Olympic construction site in London.⁸

Three elements – the push and pull of media debate, the obvious growth of the industry, and its increasingly diverse applications – provided the backdrop for a second major event in February 2009, hosted by the SMF and supported by the UK Identity and Passport Service (IPS). The event brought together academic experts, industry figures and public policy

¹ Omand, David (2009) 'The National Security Strategy: Implications for the UK intelligence community' *Institute of Public Policy Research* Discussion Paper, February 2009 p.9

² 'Meet the New Freedom Fighters' *The Observer* 22nd February 2009. Accessed at <http://www.guardian.co.uk/uk/2009/feb/22/civil-liberties-human-rights-charter88>

³ Lecture given by Jacqui Smith as part of the SMF Cabinet Lecture series, 6th November 2008. See <http://www.smf.co.uk/smith-06112008.html>

⁴ See for example 'Q&A: Identity Card Plans' *BBC Online*, 6th March 2008. Accessed at http://news.bbc.co.uk/1/hi/uk_politics/3127696.stm

⁵ 'Business Truth: Focus on Biometrics' *The Telegraph*, 12th February 2009. Accessed at <http://www.telegraph.co.uk/sponsored/business/businesstruth/3796300/Business-Truth-Focus-on-Biometrics.html>

⁶ Introna, Lucas D. & Wood, David (2004) Picturing Algorithmic Surveillance: the Politics of Facial Recognition Systems *Surveillance and Society* 2(2/3): 177-198 p.182

⁷ 'A Potted Guide to Biometrics' *The Times*, 13th October 2004. Accessed at http://www.timesonline.co.uk/tol/sport/related_reports/article493793.ece?token=null&offset=0&page=1

⁸ 'Biometrics Screening for Olympic Workers' *The Times*, 5th March 2009. Accessed at http://www.timesonline.co.uk/tol/sport/olympics/london_2012/article3486089.ece

practitioners, with the intention of digging beneath the surface and eliciting high quality debate on a poorly understood topic. What follows is a report of the proceedings.

Part I: A history of the future; a future of the history...

The event was headed by a keynote speech from Professor James Wayman, an international expert in biometrics at the Office of Graduate Studies and Research, San Jose State University and Department of Electronics, University of Kent. As well as authoring a number of key publications in this area, Professor Wayman has acted as an advisor to the US, Australian and UK governments and can draw on over 20 years experience in the field. His presentation provided a potted history, and a look into some of the key debates within the industry. He was passionate about the potential benefits of biometrics, but in a way that appreciated their strengths and weaknesses within different settings.

Professor Wayman began with an introduction to the topic, recognising that biometrics is a contested term, and also one that is shared with another (primarily British) field – the study of biological statistics. Despite some disagreement however, he argued that we can reach a basic definition.

“the automated recognition of individuals based on their physical or behavioural characteristics.”⁹

Of central importance to this definition is understanding precisely what is meant by ‘recognition’. Recognition suggests that biometrics allows humans to be recognised from their physical attributes. As Professor Wayman noted, ‘not included in the definition...are deception, intent, identity or identification. Biometrics is about recognition; who you are is another story entirely’. The relationship between biometric data, identity and privacy is thus not as clear cut as one might assume from the popular media. Biometric systems translate information about human features into code¹⁰ – the mapping of distinct identities onto this code is a separate process.

Professor Wayman then moved on to the potential uses of biometrics in security and verification systems, foregrounding some pertinent social issues. He used the example of a chip-and-pin credit card, which is designed to be both personal and secure. The card belongs to the individual, but a partner or carer could use it with the owner’s consent (and pin number). This would not be possible if identity was verified through fingerprint recognition. Similarly, we can leave a spare house key with a neighbour in case of emergency, but this is not an option if the house is protected with a fingerprint reader.

Professor Wayman argued that, for these reasons, biometrics implies a very different kind of social structure, and one that may not be appropriate for all of its potential applications. Technology such as chip-and-pin therefore does not need to compete with biometrics, especially in situations where the individual has a vested interest in keeping his or her identity safe. A counter-example is the Disney system, which demonstrates how biometric identification can be employed when the individual has no such motivation. Here, the individual is issued with a season pass that could easily be shared around multiple users. If this were to happen, Disney would lose out, as the individual would have little incentive not to share the pass. To combat this, Disney has implemented a ‘positive claim’ system using finger scanning at their Florida resort.

⁹ A slightly fuller definition is “the automatic recognition of people based on their distinctive anatomical (e.g. face, fingerprints, iris, etc.) and behavioural (e.g. online/offline signature, voice, gait, etc.) characteristics.” Kruger, Erin; Magnet, Shoshana; and Van Loon, Joost (2008) ‘Biometric Revisions of the Body in Airports and US Welfare Reform’ *Body and Society* 14(2): 99-121. P.103-04

¹⁰ *ibid*, p.104

These examples take us to the key differences between ‘positive-’ and ‘negative-claim’ systems – and the way in which they engage with biometrics. A positive-claim system ‘is to prove (one is) known to the system, to prevent multiple users of a single identity’. So, for example, the UK IRIS programme can establish the individual as a known user of the system, linked to a single, distinct identity. For Professor Wayman, this is tantamount to saying ‘you know me and no-one else can come into the country pretending to be me because the biometric is going to link me to that one identity, such that it will prevent multiple users of a single identity’.

A negative-claim system works in a different way. It relies on establishing that an individual is *not* known to the system – so that his or her fingerprints would not correspond to any existing database record. It was argued that this system leaves increased room for fraud through a potential ‘false non-match’. This could occur if an individual is enrolled within a system, but is wrongly flagged as being unknown – for example if their appearance or fingerprint had changed. One audience question picked up on the margin for error within such a system, asking whether we could ever ensure the uniqueness of an ID given that a false match rate ‘as tiny as one in a million’ could end up with ‘billions of false matches’. Professor Wayman argued that the use of multiple biometric identifiers will be key to combating this (such as using 6 or 7 fingerprints). The more identifiers one can match, the narrower the scope for error. There was disagreement in the numbers, but an acceptance that other profiling factors (such as gender) could be used as well.

These observations have important ramifications for the use of biometrics in national schemes, as the example of voter registration in the U.S. shows. Professor Wayman was consulted by the Federal Election Commission (FEC), which was concerned by instances of multiple registration and multiple voting. The FEC wanted to explore a biometric solution to this, but wanted it to be voluntary. Professor Wayman argued that this would cause a ‘big logical problem’, and that ‘a system for proving I’m not known to the system (i.e. a negative-claim) must be mandatory’. The issue here is preventing people from holding more than one identity, making it necessary for everyone to enrol in the system. This has implications for a national ID card scheme which, he argued, must be mandatory ‘if (the) purpose (is to) prevent issuance of multiple cards to the same individual’.

Weaving in and out of these examples was a warning about the way in which biometric data is collected, stored and interpreted. Professor Wayman pointed out that identity is ascribed through the *interpretation* of biometric data, and that this process is rarely error-free. For example, UK IRIS scanning might facilitate quick and easy recognition, but enrolment into the system requires identity to be verified by non-biometric signifiers – such as a passport. So, the big challenge for national schemes is not necessarily collecting the data, but rather matching it to the right people, using the previous records already held by government. To quote: ‘collecting the biometrics is easy, it’s...mapping to the previous information that you have in the system that becomes really, really hard’.

Professor Wayman expanded on this point in the subsequent Q&A session. The greatest difficulty, he argued, is in ‘mapping back to data already in the system’. People change their name (especially women); they are unsure about dates, and documentation becomes out-of-date and gets lost. In addition, those administering the system will be dealing with thousands of people with the same names – all leaving room for error, and making it difficult to match biometric data to the individual. The implication is that unless the system joining biometric data to existing identifiers is secure, then a biometric system will not necessarily be more efficient than existing non-biometric schemes.

Professor Wayman concluded his presentation by reflecting on two other ‘key issues’ in biometrics: ‘expense and complexity’. Biometric systems generally require significant capital costs and setup expertise, especially if people would need to be enrolled each time they joined a new scheme. A national ID database would, of course, make this a significantly

smoother process. Finally – and perhaps most importantly – greater thought must be given to usability. The concept of being ‘biometrically disabled’ was introduced here. For example, a crooked little finger could make full-palm recognition impossible. The vendor community must, he argued, focus on broadening usability across the wider public. This will become increasingly important as the use of biometrics increases over the next 20 years.

Part II: Comparative Perspectives on the Development of Biometrics

The debate was widened further in the panel session that followed Professor Wayman’s contribution, where four short presentations were given. The first was delivered by Dr Peter Hawkes, former Chair of the Intellect Association for Biometrics. Dr Hawkes reflected on the evolution of biometrics, from the use of inked fingerprints by the Chinese in the third century, to the development of IRIS technology today. He gave the audience the sense that the field is constantly reinventing itself, turning out new ways to address the social needs of the time.

The link between biometric technology and social need is key to understanding the directions the industry has taken. For instance, the development of fingerprint recognition was given impetus by the Metropolitan Police, who first established a fingerprint branch in 1903. More sophisticated methods – such as facial recognition – have been developed in pace with the emergence of new technologies. And as the ways in which we interact and transact with each other evolve (e.g. through internet and mobile communications), new ways of verifying identity will continue to be required.

To this end, Dr Hawkes shared his ‘personal dream’ of speaker verification. ‘Because it is favoured by a very low cost, good quality microphone’, he argued, ‘the potential for mobile commerce and e-commerce is enormous’. This is one way the industry could go, but to make bold predictions would be foolish. ‘What seems impractical today’, he argued, ‘may be economic tomorrow’.

Dr Hawkes was followed by Hugh Carr-Archer, CEO of Aurora Computer Services. Aurora is ‘the UK leader in the provision of face recognition technology’.¹¹ As such, Mr Carr-Archer was well placed to discuss some of the applications of biometrics from a commercial perspective. He began by talking about the use of face recognition technology in the construction industry. Wage fraud is a big issue for employers, and face recognition technology makes it possible to combat this by eliminating ‘ghost’ workers from the payroll, and ‘double dipping’¹² by employees. He noted that a trial of its use with one large construction company brought a 6% reduction in their wage bill.

Mr Carr-Archer also highlighted a recent pilot project in a 6th form college, which has employed face recognition technology to register pupil attendance. The scheme has saved teachers from taking a manual register, so their time can be put to more profitable use elsewhere. This is a fairly clear benefit, but also one that generated a good deal of controversy. Media attention in this case focused not on the potential positives of the pilot, but on issues of privacy and security. ‘How do you think people will react to having their biometric data stored? How are you going to protect them? What happens if the data gets lost?’ Mr Carr-Archer’s examples provide a microcosm of public debate on biometrics.

¹¹ See Aurora homepage at <http://www.facerec.com/>

¹² Double dipping refers to the use of multiple identities by a single person, or in this case falsely clocking on as someone else as well as yourself. See Van der Ploeg, Ima (2003) ‘Biometrics and Privacy: a note on the politics of theorizing technology’ *Information, Communication and Society* 6(1): 85-104

Such questions are of course valid ones, and Mr Carr-Archer suggested that it is incumbent upon the biometrics industry to make sure that ‘encryption, communication channels (and) safety’ are foregrounded in their concerns. One key element of this is making sure that ‘reverse engineering’ is not possible, so that identity cannot be established from compromised biometric data (if a dataset is lost or stolen, for example). Such attention to personal security will inevitably push up costs in the first instance, but the long-term benefits could more than outweigh this.

The third speaker was Toby Stevens, Director of the Enterprise Privacy Group (EPG). The EPG is an association of organisations aiming to ‘understand privacy and identity-related issues and to achieve collaborative solutions’¹³. Accordingly, Mr Stevens spoke on the topic of ‘privacy laws and individual freedoms’, highlighting what he saw as the ‘incredible potential’ of biometrics to infringe on privacy.

Mr Stevens began by talking about personal sensitivity, and the way in which biometric data can convey information that the user may not themselves choose to make available. There is a blurred boundary, he argued, between consenting to the use of specific personal data, and the ability of biometrics to infer other, related information. The sharing of biometric data across government departments (as mentioned above in the context of the Omand report) is one way in which privacy can be violated through this process. Trust and consent must be built between the public and the industry to address these fears, and this can only be done through the appropriate and judicious use of biometric systems. ‘In the rush to adopt biometrics’, he argued, ‘we have seen disproportionate applications of the technology’.

Mr Stevens then spoke about the relationship between identification and authentication. ‘In the vast majority of cases’, he argued ‘we use biometrics to *authenticate* an individual. Is this the legitimate card holder? Is this the person they’re asserting that they are?’ This is different from marking someone out – determining that they are a single identity within a large population. He questioned the need to *identify* rather than authenticate in the case of UK IRIS, holding that binding individuals back to a machine-readable passport was more reliable and more practical.

Mr Stevens concluded with the suggestion of a ‘privacy impact assessment’, to which every biometric application would be subject. This would consider the context within which biometrics are used, whether they are a proportional response to the issues concerned, and would ensure the correct safety measures are implemented. This would be a means of fostering public trust, and making sure that biometric applications can be developed within a secure framework.

The final presentation was given by Dr Farzin Deravi, Department of Electronics at the University of Kent. Dr Deravi provided an academic perspective on biometrics research, and the challenges ahead for those developing new technologies and new ways to use them. He began by asking a broad question of the industry: ‘is biometrics really ready, or not?’ We have seen a fantastic amount of progress in certain areas, but biometric systems are still vulnerable to data misuse in a number of ways. In response he urged a holistic approach to new research that privileges the development of technologies to meet real social needs, and an overall emphasis on responsibility for those designing and deploying these technologies.

¹³ See EPG homepage at <http://www.privacygroup.org/>

The presentation also focused on the idea of multiple biometrics. Can we increase safety and efficiency by combining biometrics (for example using a thumb and a finger, or face and voice)? Research in this area should be mindful of the whole population, not just the mainstream. Dr Deravi used the biblical story of Isaac, who was old and blind, to illustrate this point. We need to make sure that biometrics does not disadvantage such people, and make sure that new technologies are developed with varying degrees of adaptability in mind. If this can be achieved, the industry has the potential to ameliorate real social problems in the future.

In sum, Dr Deravi laid out two possible futures: one, in which biometrics are used gainfully and safely, enhancing our lives and making everyday tasks easier; another, in which trust in the field is eroded by data vulnerability and misuse. Future biometrics research must walk this tightrope, and make sure the advantages outweigh the drawbacks.

The presentations were followed by a Q&A, in which audience members followed up on some issues of interest. This part of the session showed how the audience had found the event stimulating and thought provoking. The way in which further conversations continued afterwards suggested there could be a need for further debates to tackle the issues arising from the discussion.

Overall the event highlighted that whilst developments in efficiency, security and usability that biometrics could bring may be beneficial, this has to be balanced against the potential for data misuse, which can ultimately have human consequences. The future of biometrics must successfully negotiate this moral maze.

Event contributors:

Chair - Ian Mulheirn, Director, Social Market Foundation

Speakers:

Professor James L. Wayman,

Department of Electronics, University of Kent and Office of Graduate Studies and Research
San Jose State University

Dr Peter Hawkes

Former Chair of IAFB

Hugh Carr Archer

Aurora Computer Solutions

Toby Stevens

Director of the Enterprise Privacy Group

Dr Farzin Deravi

Reader in Information Engineering and Director of Research, Department of Electronics, University of Kent

Event Attendees

Aidan Littlewood	Lockheed Martin
Alasdair Darroch	Biostore Ltd
Alex Bazin	Fujitsu
Ann Symonds	ASG Immigration
Asavin	
wattananjantra	Dennis Publishing Ltd
Aziz Shaikh	UniversalSoft Ltd
Ben Fairhead	Lockheed Martin
Ben Vogel	Jane's Airport Group
Brian Wheeler	BBC News
Dan Worth	BAPCO Journal
Daniel	
Rosenstone	Weber Shandwick
Dave Birch	Consult Hyperion
	Parliamentary Office of science and technology
David Cope	
David Moss	Business Consultancy Services Ltd
David Watkinson	IPS
Dean Fell	IPS
Dermot Kehoe	IPS
Dorothea Hodge	SMF
Edwin Ballo	Logi
Fred Piper	Royal Holloway University
Fred Preston	Motorola
George Gallimore	Police Federation
Hilly Janes	Wired Magazine
Ian Mulheirn	SMF
Jackie Lepoidevin	Facilities Management
Jim Lound	Experian
Jonathan Rush	Contingency Today
Keith Ryan	Caspian Publishing
Laura Tomlinson	SMF
Lee Hibbert	Professional Engineering Magazine
Liz Hodges	Logi
Lord Errol	House of Lords
Lucy Grove	Grayling
Mark Say	GC Magazine, Kable
	Parliamentary Office of science and technology
Martin Griffiths	
Mazin Zeki	
Michael Clark	G4S
Michael Macmillan	Home Office
Mztkowska Milena	Logi
Neal Weston	British Air Transport Association
Patrick Stutt	Home Office
Paul Stanborough	Aditech
Paul Wilson	De La Rue
Richard Mabbott	APACS
Ruwan Kodikara	Tetra Strategy
Sally Dobson	SMF
Samina Choudary	IPS
Saskia Walzel	Consumer Focus
Spencer Chapman	Post Office
Steve Bannister	Avail Consulting
Will Hoyles	SMF

The Social Market Foundation

Director

Ian Mulheirn

Board Members

Lord Lipsey (Chair)
Viscount Chandos
Gavyn Davies OBE
David Edmonds CBE
Daniel Franklin
Martin Ivens
Graham Mather
Brian Pomeroy CBE

Policy Advisory Board

Lord Adebawale CBE
Wendy Alexander MSP
Professor Nicholas Barr
Liam Byrne MP
Dr Vincent Cable MP
Philip Collins
Simon Crine
Don Cruickshank
Lord Dahrendorf KBE
Ed Davey MP
Evan Davis
Alan Duncan MP
Daniel Finkelstein OBE
Liam Halligan
Lord Haskins
Nick Herbert MP
Sir Peter Lampl OBE
Dr Oliver Letwin MP
Maria Miller MP
George Osborne MP
Lord Parekh
Trevor Phillips OBE
Lord Plant
Sir Stephen Sherbourne CBE
Sue Slipman OBE
Lord Stevenson CBE
John Tizard
Lord Turnbull KCB CVO
Stephen Twigg
Andrew Tyrie MP
David Willetts MP