Surveillance & Society

Article

Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology

Jonathan Bright

PhD Candidate, European University Institute, Italy. jonathan.bright@eui.eu

Abstract

If surveillance technologies are to be democratically controlled, then knowledge of these technologies is required. What do they do? How do they work? What are the costs? Yet gaining this knowledge in the context of a new surveillance technology such as biometrics can be problematic, because no settled definition exists. Competing versions of biometrics appear in both public and governmental discourse on the technology: different ideas about how often it fails, where it can be used and even what it does. This paper is an exploration of how these different versions compete with each other, and how knowledge about a new surveillance technology such as biometrics is thus constructed. Through reference to original research in the context of the use of biometrics in the UK, points of stability and instability in the definition of biometrics are identified, and some of the processes through which instable definitions become stable are tracked.

From this empirical story, conclusions are drawn both for the process of construction of the meaning of technologies, and the general practice of surveillance in modern society. In particular, this paper aims to show how notions such as democratic control (central to the legitimation of state surveillance) become problematic when the very meaning of a technology is negotiable.

Introduction

Over the last 10 years, the UK government has invested heavily in biometric technology, making it the key component in a range of upgrades to government identity systems: most significantly in biometric visas, biometric passports and of course the (eventually cancelled) biometric National Identity Scheme [NIS]. These systems, especially the NIS, have been highly controversial, provoking fierce debate both within parliament and amongst the public at large (for an overview of the NIS debate see Whitley and Hosein 2009). Whilst the government has been keen to position them as tools for combating identity fraud, illegal migration and (perhaps most of all) terrorism, opponents regard them as evidence of increasing government surveillance, where the life of the everyday citizen becomes subject to ever increasing intrusion and control.

The legitimacy of these systems relies on the idea that they are democratically controlled: they are created by democratically elected governments (and by extension the population at large), and overseen by these governments or bodies to whom they delegate responsibility. However, this legitimacy suffers from a problem of knowledge created by the new technologies used in these systems, of which biometrics is a prominent example. In order to govern a technology, knowledge of the technology is required; but in the case of technologies such as biometrics, gaining this knowledge can be problematic. Part of the problem is

Bright, Jonathan. 2011. Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology. *Surveillance & Society* 9(1/2): 233-247.
http://www.surveillance-and-society.org | ISSN: 1477-7487

that the technology is complex, and a degree of expert knowledge is required to understand it. But perhaps more important is the fact that finding this expert knowledge is itself problematic, because no settled definition of the technology exists. There is no one source of expertise which government can consult before deciding whether to use a technology. Rather, a host of competing versions of biometrics exist: different claims about how accurate it is, how intrusive it is, even what it should be properly used for. Furthermore, these versions themselves are not static, shifting both as the debate continues and as biometrics itself is deployed.

These controversies are typical of an emerging technology, and point to a basic premise which has emerged from science and technology studies: there is no separation between technology and society (Hughes 1986). Technologies 'do not...evolve under the impetus of some necessary inner technological or scientific logic' as Bijker and Law put it (1992, 3). Biometrics is not something which exists outside of society, a piece of technology waiting to be discovered and applied. Instead, its meaning is constructed through its application. As biometric systems are built, definitions of biometrics are also built; knowledge about biometrics is as constructed as the technology itself. Therefore, as biometrics is yet to be widely applied, knowledge about it is still being constructed, and its meaning is thus 'flexible' (Bijker 1995). This is not a radical observation; indeed, it is something that the entire biometrics industry is acutely aware of. In the UK uses of biometrics such as the on-going ePassports programme are in the process of defining knowledge about biometrics. If they are perceived as successful, other biometrics applications will be boosted. If they fail, the government may never again invest in the technology, and the private sector could follow suit (see Heath 2005).

This problem of knowledge is also something that affects those wishing to study biometrics. Faced with this multiplicity of representations, the analyst of biometrics has two options. They can try and decide for themselves which version is closest to the 'truth', and then analyse the extent to which this truth influences the thinking of policy makers. Or they can stand back, try to remain agnostic towards true and false definitions, and instead study the processes through which these definitions are contested (this approach has been labelled the 'empirical programme of relativism' – see Collins 1981). There is nothing wrong with the first approach (though more radical constructivists might regard it as ultimately doomed to failure): indeed, as I shall argue below, any hope of democratic control of a technology relies on people's ability to try and construct some type of knowledge about it. This paper, however, takes the second option, in the belief that studying the processes by which debates take place can be just as political as entering into the debates themselves. In particular, by exploring how knowledge about biometrics is formed, the aim of this paper is to point to ways in which technologies such as biometrics can be democratically controlled in spite of fundamental uncertainties about what they are.

Technological Knowledge and Democratic Control

Sheila Jasanoff argues that "democratic theory cannot be articulated in satisfactory terms today without looking in detail at the politics of science and technology" (2005, 6). There are many aspects to democratic theory, and hence many areas where these politics matter. The focus of this paper is on the legitimacy provided to technology by the democratic control of its use.

As Jasanoff highlights in her discussion of the politics of stem cell research, legitimacy can be conferred on any given technology if its use is controlled through a democratic process (2005, 2). These processes can themselves be quite diverse, and of course vary between different democracies and different issues; hence there is a wide range of different types of legitimacy and control. Most obviously, a government gains a kind of background legitimacy simply through its ability to win general elections. More specifically, legislative assemblies provide legitimacy by scrutinising individual bills or allowing space for public debate of important issues. Courts provide legitimacy by providing a venue for legality to be debated after legislation is passed, while a host of independent or semi-independent bodies (such as Data

Protection Agencies) may also provide legitimacy through reviewing policy or imposing sanctions. Finally, the public at large provides some kind of legitimacy by supporting or opposing particular measures, opinions which filter back in a variety of different ways to elected representatives.

However, while the types of process may be manifold, the starting point of this paper is that "knowledge" of technology is vital to the functioning of all of them, and hence central to any notion of democratic control. It seems self-evident, for example, that for a parliament or congress to debate the merits of a technology they must have at least some information about what it is and what it does. As I argued above, however, especially in the case of an emerging technology, gaining such knowledge can be problematic.

This paper takes an approach to technology and technological knowledge based largely on actor-network theory (see Latour 2005 for an overview). Biometrics is conceptualised as a 'actor-network': a series of related actors out of which the technology forms. The technology itself forms part of the network: physical machines which capture fingerprints or compare iris patterns. But so do the people who use these machines, and the environments in which they are positioned. Furthermore, knowledge about biometrics also forms part of the network: assumptions about how well the technology works *act*, in the sense that they will condition where and how it is used.

Knowledge about a technology can be divided into two types: facts and controversies. Facts are pieces of stable knowledge, widely accepted as representing some kind truth (see Latour and Woolgar 1979). An example would be the statement: 'fingerprints represent a type of biometric'. Controversies are points where the definition of biometrics is 'flexible' (Bijker 1995[1]), where multiple definitions of biometrics exist. An example would be the question: 'how accurate are fingerprint biometrics?' The aim of this paper is not to try and settle these controversies, but rather to look at how they come to be settled, and thus explore how knowledge about a complex technology such as biometrics is built.

How can facts and controversies be identified? Actor-network theory [henceforth ANT] recommends looking for disagreement, for open contestation of bits of knowledge as a sign that they are not yet facts (Callon 1986, 204), or the existence of qualifying modalities attached to particular statements, such as 'it is claimed that...' (Latour and Woolgar 1979). These discourse based ways of defining controversy are appropriate to the general ANT principle that action should always leave a trace (on traceability see Latour 2005, 193). However, it is important to note the potential this methodology has to marginalise powerless actors, who may disagree but are unable to contest particular definitions (Russell 1986, Winner 1993). Therefore, the definition of a 'fact' here does not necessarily imply a universal consensus, but merely an absence of contradiction in the research conducted.

This research took place as part of a wider project investigating the development of public identity systems in the UK, especially the National Identity Scheme which the Labour government tried to implement in the period 2001 - 2010. This paper therefore concentrates on applications of biometrics to such identity systems. Interviews and documentary analysis were the two techniques used to gather empirical evidence. Interview candidates were collected in the first place by identifying the government bodies, campaigning groups and other institutions which had a high profile involvement in biometric projects such as the National Identity Scheme; this list was augmented by 'snowballing' (Bijker 1995) at initial interviews to identify those whose involvement was less obvious. Documents were collected by systematically studying the published output of the institutions and groups identified as being important to the meaning of biometrics in the UK. Both the facts and the points of controversy reviewed here were selected on the basis of these interviews and documents.

[1] I should note that Wiebe Bijker's work sits somewhat outside actor-network theory, forming part of an alternative programme sometimes called the "Social Construction of Technology". The differences between the two schools are however not relevant for this article.

So, what are the facts about biometrics? What pieces of knowledge are stable? A 'biometric' is a measurement extracted from the body and then stored in a certain format, which can be compared to measurements previously extracted from the same body. The word 'biometrics' refers to the technology or set of technologies which enable this measurement and comparison, and also allow for the integration of this process into systems which rely on being able to distinguish between different bodies. Biometrics, in this sense, is an umbrella term for a family of technologies which may have quite different implementations (for example, DNA comparison and voice print analysis are both biometrics, yet require very different machinery).

Biometrics as such has a relatively short history, especially in public identity systems. While techniques such as anthropometry (measurement of parts of the body) and fingerprint classification were experimented with by various branches of public administration around the beginning of the 20th century (see Kaluszynski 2001, Sengoopta 2003), it was not until the 1990s that governments began to seriously consider the use of biometrics in large scale public identity schemes. Within these systems, biometrics are typically called upon to perform either 'authentications' (a 1:1 comparison of a biometric template held on file with a biometric taken from a person, to establish that person is who they claim to be) or 'identifications' (a 1:n comparison of a biometric taken from a person with all other biometrics on file, to establish if that person exists in the database). Such systems are of course not the only possible applications of biometrics. One of the original aims of Francis Galton, developer of an early fingerprint classification scheme, was to use biometrics as a way of pursuing eugenic profiling of humans (Sankar 2001). Fingerprints and DNA are also used very widely in criminal justice (Cole 2001), while today people are even experimenting with the use of biometrics to detect mood, and even personal associations. These uses are however beyond the scope of this paper.

Even if these basic facts about biometrics are accepted, many pieces of knowledge about the technology remain unstable. During the research conducted for this article, three particular points of controversy were identified: whether biometrics is an intrusive technology, and if so when its use is proportional; whether biometrics is a technology that 'works', and if so how accurate it is; and what biometrics 'does', what its functions are. All of these points of controversy are important in processes of democratic control. The aim of the rest of this paper is to explore these three points of controversy: charting the different possible visions of biometrics which exist, some of the venues where these visions compete, and some of the processes by which points of controversy stabilise and knowledge emerges.

Constructing Proportionality

The concept of 'proportionality' is often employed in democratic debate surrounding the use of technology, especially technologies which impose costs as well as benefits. Many democratic processes which regulate technologies either implicitly or explicitly refer to some notion of the proportionality of the technology in question. Tracing how a society decides when a technology is proportional is, however, an extremely challenging task. Like identifying settled controversies, determining what actors think about the normative implications of a technology is methodologically problematic, especially when that technology is unstable. As work on science and technology studies has shown, the proportionality of a technology in a society is something that can shift over time or with experience. The use of fingerprinting in criminal justice, for example, was considered by some to be a gross violation of the rights of the accused when it was first deployed around the turn of the 20th century. Now it has become normal practice (see Cole 2001).

The most obvious way of tackling the question is to look at parts of society with explicit responsibility to consider these issues: here, proportionality will leave traces. One such body in the UK is the Information Commissioner's Office [ICO], which has responsibility for the enforcement of the UK Data Protection Act. This act provides a number of basic 'data protection principles' (Schedule 1 Part 1), among which principle 3 is particularly relevant: 'Personal data [of which biometrics is a type] shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed'. Looking at the application of this principle is one way of examining how a society such as the UK exerts control over a biomerics by determining when it is and is not 'excessive' to use it (i.e. proportional).

During the course of research, two ICO opinions which were based specifically on biometrics came to light. The first is how the ICO used their influence to halt proposals for a fingerprint based access control system to a new passenger lounge at Heathrow (for some background see Privacy International 2008). This case emerged during interviews conducted with two ICO staff members: Iain Bourne (Head of Data Protection Projects) and Lyn Wibberley (Senior Data Protection Development Manager)[2].

> Bourne:
>
> 'there were obvious cases such as the Heathrow terminal fingerprinting thing...they were going to bring in a system of fingerprinting for all passengers using one of the terminals at Heathrow so that all passengers could use a shared departure lounge, which would allow them to have access to more shops, which we thought was a very weak argument in terms of taking what is quite an intrusive biometric'
>
> Wibberley:
>
> 'our main point was, if you were just getting on a flight from London to Manchester, is it necessary to have your fingerprints taken? And the reason that they did that was one of security, because they had created this thing [the shared departure lounge] and then didn't know how to manage it'
>
> 'it was just about to be deployed...all the equipment was there and everything. That was stopped at the last minute. I think that shows that when you do things like starting to fingerprint passengers who you wouldn't have fingerprinted before you have to think through all the issues'

The second is an opinion issued by the ICO on the use of biometrics in schools (Information Commissioner's Office 2007). Roughly 10% of schools in the UK are using biometrics for a variety of purposes: to track attendance, monitor the use of libraries, secure school meal payment systems, etc. (Infosecurity 2009). The opinion is interesting because it makes no reference to the third principle mentioned above. The ICO did highlight areas of concern, saying in particular that data should be collected with the informed consent of children, and in such a manner that makes it difficult to reuse in other biometric systems. They also highlighted the need to store that data in a secure manner, and the concern that fingerprinting might make children 'feel like criminals' (though they note that this last concern is beyond the scope of the DPA). However, there is no real mention of proportionality, no in principle objection to the use of biometrics in a school environment.

The aim here is not to suggest that the ICO is being inconsistent. These two cases are only comparable to a certain extent: one was a high profile initiative, where the ICO worked with full knowledge of the system and what was at stake; the other is a very short, general opinion. It is perfectly possible, if asked for some reason to consider a specific biometric system in a specific school, the ICO might still consider that principle 3 was relevant. The ICO is anyway not a body responsible for assessing the proportionality of a

[2] Interview conducted on the 8th of September 2009.

technology per se; they deal with technology only inasmuch as it has implications for personal data. They are therefore under no obligation to adopt a fixed position on biometrics in abstract.

Instead, the aim is to show is that at least two different possible visions of the impact of biometrics as a technology exist. The first, emerging in the Heathrow case, is of a technology that is only proportional in certain circumstances. Here biometrics (especially fingerprinting) are potentially intrusive, and not justified solely for the provision of better shopping facilities. The second, in the schools case, seems to point more to a technology that is generally acceptable to be deployed throughout society. Here there is no in principle objection to their deployment in a mundane, routine environment such as a school canteen.

Interestingly, this dual definition of biometrics (something normal / something exceptional) is something that exists in the wider debate about the place of public identity systems in the UK. As the National Identity Scheme was formed in the aftermath of 911, a strong public association exists between the idea of ID cards and the need to take emergency security measures. This association was helpful in enabling the initial materialisation of the scheme, however has also been slightly double edged. A scheme justified on the grounds of security will appear, almost by definition, to be disproportionate in a context when security is not at stake (it is worth noting that a previous UK identity system, constructed during World War II, was dismantled because it was no longer seen as acceptable in a time of peace - Home Affairs Select Committee 2004, 9, see also Thompson 2008).

The government, perhaps aware of this, has tried to resist this total ‘securitisation’ of the scheme (Buzan, Waever and de Wilde 1998); trying, in frequent public interventions, to normalise the NIS, to position it as something mundane. For example, Home Office minister Andy Burnham said, in 2006: ‘I take the view that it is part of being a good citizen, proving who you are, day in day out’ (Guardian 2006). Charles Clarke, Home Secretary at the time of the passage of the ID cards bill, equated ID cards with other routine pieces of ID such as ‘cash and credit cards, driving licences, passports, work security passes and any number of the other current forms of ID that most of us now carry’ (Times 2004). Furthermore, in ID card planning documents, the scheme was conceptualised as something that would become ‘part of everyday life’ (Home Office 2006).

This example also shows the difficulty that regulatory bodies such as the ICO have of assessing the impact of technologies like biometrics through reference to principles like proportionality. In both cases, it is fair to say that the ICO exerted control over the technology: they judged its costs and benefits, reached an opinion, and (in the Heathrow case) prevented its use. But in neither case can we say that proportionality was the basis of this control, because in each case, the same technology appeared to have a different impact.

It is not clear which definition of biometrics (normal or exceptional) will stabilise. This is something that will also depend on how and when it is used. Technology can be defined as normal or exceptional through public debate, but it can also become more normal through routine use (as in the example of criminal fingerprinting above). The ICO schools opinion included this possible objection to the use of biometrics in schools: ‘it has even been suggested that fingerprinting in schools is part of a concerted attempt to “soften up” the younger generation for increased state privacy intrusion, including initiatives such as ID cards and DNA testing’ (Information Commissioner's Office 2007, 1). Therefore, when biometrics becomes deployed in normal circumstances, away from airports and connections of terrorism, it can help it become considered as a mundane technology. In this way, proportionality can be constructed alongside biometrics systems, and can be thought of more as a *result* of this process of construction, rather than something that allows the process to begin.

The difficulty of using proportionality is something Bourne and Wibberley were keen to highlight. As Bourne said (of the Heathrow case):

> 'I think that shows the difficulty of attempting to balance a passenger's wish to have better shopping facilities, and the airport's need for revenue, against personal privacy. You can't do it – you need a different way of looking at these problems, personally I don't think talking about balance or proportionality gets you very far'

He continued:

> 'there's not a science to this really [assessing things like privacy, proportionality]...there are no [objective] values you can use to measure privacy against technological intrusion... you've got to look at it and say well, to the police or whoever it is, right, why do you want to collect that information? ...and the police may well come to us and make a convincing case that the deployment of a new technology is for the social good and that their collection of information is therefore justified'

The ICO, in other words, works on a case by case basis, rather than through reference to abstract values. This is an efficient solution to the problem of defining proportionality in the case of a technology such as biometrics, but also something that serves to highlight an issue in the democratic control of surveillance technology. In a legislative venue for instance, when debating time is limited, politicians do not have the time or resources to consider the application of technologies case by case. In this context, general principles such as proportionality provide conceptual means of controlling a technology. But when proportionality itself is flexible, the extent to which the concept can be used to control a technology becomes debatable.

Constructing Success and Failure

Whether a technology is judged successful or a failure is clearly important for the notion of control. A democratic government (or indeed any government) should want to use technologies that *work*, that do what they are supposed to do. However, as much literature from science and technology studies has shown, the success or failure of a technology is ultimately just as constructed as whether it is proportional or not.

This construction has occurred in a variety of different ways, one of the most important of which for the technology being discussed has been testing, a practice which has itself attracted a lot of literature (e.g. Latour 1988, Gooding, Pinch and Schaffer 1989, Vincenti 1990). As Latour has noted, testing serves two functions: it can explore the properties of a particular device, but also be used to display these properties to whoever is able to observe them (Latour 1988, 85). This dual function of testing has proved significant in the case of biometrics.

In their 2003 planning document, the Home Office set out plans for both the legislation and implementation of the NIS. Among these plans they stated:

> 'a 6 month biometric pilot…will shortly be run by the UK Passport Service to test the recording of face, iris and fingerprint biometric information' (Home Office 2003, 5)

The results of this trial (see United Kingdom Passport Service 2005) appeared to show an extremely poor performance for biometric "authentication" (the act of comparing a person's biometrics with biometrics they had previously stored on the system – see United Kingdom Passport Service 2005, 25). These authentications were successful 91% of the time when based on iris patterns, 81% of the time when based on fingerprints, and only 69% of the time when based on facial recognition.[3] These levels of performance are clearly well below that needed to support a NIS which was supposed to engage in thousands upon thousands of such verifications every day.

However, interpreting the results of any sort of test is a political act, and can stimulate significant controversy, as the results of the test (once accepted as fact) will change the technology significant ways. This is especially true of technologies which are tested infrequently, such as nuclear missiles (MacKenzie 1990), and in this case the *en masse* use of biometrics. Furthermore, tests rely on previously constructed knowledge about what can be tested, and how (Constant 1980, MacKenzie 1989, see also Haggerty 2009 for a discussion of evaluation in the context of surveillance). A test will only be effective it is perceived to be fair.

Here it is worth exploring briefly how biometric authentication worked in this test (see United Kingdom Passport Service 2005, 25-7). In the test, images of a person's fingerprints, face, and at least one iris were captured by different imaging devices in an enrolment booth. These devices then attempted to transform the images into biometric ‘templates’, which are produced by converting various significant characteristics of the biometric in question into numeric format. There are multiple ways of doing this, but an example would be to count the number of ‘ridge endings’ in a fingerprint: areas where the ridges that form the fingerprint pattern stop or break into two.

When this process was completed, the participant moved on to a verification booth. Here again biometric samples were collected, turned into templates, and compared to the ones just taken to see if they ‘matched’, which is done on a statistical basis. As already noted, the results were poor; but the UKPS, in conjunction with ATOS Origin (the consultancy firm which ran the trial) claimed that these results did not themselves demonstrate an underlying problem with the technology. They argued that the intention of the trial was not to test the technology per se, but was instead to assess customer experience with the enrolment and verification process. The poor authentication results they explained through reference to a variety of mitigating factors (United Kingdom Passport Service 2005, 55). For example, the angle of lighting was a significant factor in facial verification: if it reflected off glasses or the person's forehead, this could hinder the verification process. Some of the trial centres were located in buildings with high windows. As the sun moved during the course of the day, its light interfered with the trial. However, this interpretation of the trial did not reach wide acceptance. Media coverage was extensive, and highlighted the negative verification rates, whilst NGO groups such as No2ID, and the Tory opposition party, both deployed the figures as arguments against the overall NIS scheme (see e.g. BBC 2005, Telegraph 2005a, 2005b, No2ID).

There are three principle conclusions worth drawing from this short study of one process by which success and failure are constructed. The most obvious is that a technology cannot be separated from its environment. The sun becomes an actor in the network when its light interferes with the process of authentication. More important for my purposes, however, is the way these actors form part of the definition of biometrics. As Latour has noted, relations between actors are not neutral: they will transform whatever they transmit (Latour 2005, 37). This is clear from the way this trial was interpreted in the public sphere. In the case of the ATOS trial, the results presented were largely accepted by media and opposition, yet the mitigating factors associated with these results were ignored or marginalised. The principle reason for this was the perception that, as the government was politically tied to the scheme, it had an incentive to present the technology associated with it in a positive light, and hence its arguments about mitigating factors could not be believed. There is nothing particularly faulty with this line of reasoning, but it serves

[3] These are the results for the group of participants who had been selected as statistically representative of the UK as a whole. Other groups of participants had different (though comparable) results. See p8 for a breakdown.

to highlight a problem for democracy: if sources of information will only be trusted when they are perceived to be acting against their own interests, then the amount and quality of information that enters public debate will be limited.

Finally, this story offers further evidence that in large scale trials of controversial technologies, the two functions of testing become mixed. Whilst, practically speaking, the realisation that biometric enrollment needs to take place in windowless rooms to be effective is a useful piece of knowledge about how technology functions (as future deployments can take this into account), politically speaking the impact of this knowledge was to make the implementation of biometrics less likely, because biometrics came to be perceived as a failure. The Home Office was clearly aware of this dual nature of testing during the course of the NIS, and ran no further public technology trials (House of Commons Select Committee on Science and Technology 2006, 36). This prevented further negative publicity about the biometrics element of the scheme, but also left these figures somewhat unchallenged in the public sphere. The difficulty of producing public evidence on the functioning of a complicated technology like biometrics is a further factor that impedes democratic control of the technology.

It is worth noting as well that evidence for the success or failure of biometrics in the context of the NIS will be attached (to an extent) to all biometrics projects. This is something the biometrics industry itself is very aware of. For example, Bori Toth, a biometrics expert employed by Deloitte at the time of the trial, said the following:

> ‘The danger is of course that people will not make the distinction between the weaknesses of the hardware [deployed in the test] and the technology itself and simply say that the stuff is not working. Even worse, making the public upset might lead to a general reluctance [to use] biometrics because of some operational problems that could have been avoided in the first place’ (cited in Heath 2005)

In this way, the debate about any particular instance of a technology serves to construct wider knowledge about all possible future instances.

Constructing functions

Even more than knowledge of its proportionality, or knowledge of its accuracy, knowledge of the function of biometrics appears to be a *sine qua non* of any kind of meaningful control. Before knowing whether to use a technology, a society must know what it does.

Problematizing the functions of a technology is challenging because technologies often appear to ’naturally’ fulfil a particular function. In fact, as many studies of technology have shown (e.g. Bijker 1995), the functions of a technology are as constructed as the technology itself. Constructing functions involves a complicated process whereby users of the technology are defined (Oudshoorn and Pinch 2003), markets are established, alternative definitions are silenced, etc. Constructing the functions of a technology is like constructing a fact: once they are built, they appear to be a natural property of the technology, and the process of their construction can be forgotten.

The biometrics systems being discussed here emerged in the UK to fulfil a security need. The conceptual linkage between identity cards, biometric passports and terrorism is quite clear in both public discourse and what is known about the government’s private thinking surrounding identity cards just after 911, especially that of the then Home Secretary David Blunkett, one of the principal architects of the NIS. For example, in a cabinet meeting on 12 September 2001, Blunkett proposed ID cards for asylum seekers, highlighting this three-way connection between terrorism, foreignness and identification (Campbell 2007, 564). Furthermore, in one of the first public airings of the plans for the National Identity Scheme following 911 (on 23 September), Blunkett discussed ID cards in the context of what action the UK should take in the war against terrorism (BBC On the Record 2001).

Biometrics therefore appears, at face value, a 'security' technology, particularly one for combating terrorism. However, in the course of research for this article, an alternative possible use of biometrics emerged: not something that increases the security of an identity system, but something that increases its speed[4]. The distinction between biometrics for speed and biometrics for security is not obvious because both functions will be implemented in similar fashions (biometrics will be used at the point of access either in a 1:n comparison with a database, or, more commonly, a 1:1 comparison with an identity document). However, the crucial differences between the two are the acceptable rate of failure, and the status of the 'secondary system': the part of the identity system which deals with people whose biometrics do not match.

Consider the example of the use of biometrics for access control. A biometric system could be installed on a gate which checked the biometrics of those wishing to enter automatically. Anyone can pass through the gate if their biometrics are matched successfully. Those whose biometrics do not match will have to enter some kind of 'secondary' identity check, and it is the way this secondary check works that determines how the overall system functions. A biometrics system designed for security must make this secondary check a stringent one. Those rejected by the system might go through a long interview, or a background check. Perhaps they might be refused entry entirely. The function of biometrics in a security system is therefore to place suspicion on those people who fail a biometric check, and to justify the intrusion of a more secure inspection. The "cost" of this security system will grow as the error rate of the biometrics increases. As more false rejections are made, more and more innocent individuals will pay the price of this security.

A biometrics system designed for speed, however, is not obliged to make this secondary check any more secure. Regardless of the secondary system, a biometrics system will increase the speed of the overall access control process if a good proportion of individuals can pass through it successfully, simply because the machine should check biometrics quicker than a human checks identity documents. The function of biometrics in a speed system is therefore to replace human document inspectors. In this situation, it is worth noting, the system overall may even be less secure than a gate based solely on human checks, as anyone trying to trick the system will essentially have two chances: they will be able to first try to trick the biometrics, and then next try to trick the secondary system. However, any individuals who are attempting to defraud the system will be mixed in with those whose biometrics simply have not functioned correctly.

The status of the 'secondary system', i.e. what happens to an individual if the biometric check has failed, is therefore a useful indicator of the intentions of the designers of the system. It will indicate in particular how accurate they consider the biometrics to be (i.e. how many innocent people will be caught by it), and how important they consider the security function of the gate to be (i.e. what is the cost of failing to spot someone who defrauds the system?).

In the UK, biometrics has oscillated between these two definitions, in a similar way to its oscillation between routine, everyday technology and exceptional security measure. In particular, pre-911 saw a focus on biometrics for speed, which shifted post-911 to biometrics for security. This is now drifting back

[4] Here I should emphasise again that I am looking at biometrics only in the context of identification systems. Still further applications such as eugenic classification, mood prediction etc. exist or have been suggested, but are beyond the scope of this study.

towards to biometrics for speed. This is something that emerged during an interview with Professor Angela Sasse[5], who said the following:

> ‘there is a very clear post 9/11 factor to this…and it was very interesting because of course with the biometrics roadmap project [a report on biometrics co-authored by Sasse], this was pre-911, and actually when I wrote my report then I said…if there is wide deployment and growth of this stuff [biometrics] it’s going to be in the private sector and it’s about convenience, convenience, and more convenience for individual customers/citizens, and business process improvements for organisations. It’s not about higher security. If you have high security requirements and a large user base, it's very difficult and expensive to make it work well - and the will to invest the necessary time and resources into the “tuning process” is not there’

If biometrics was being considered in speed terms before 911, It is evident that its adoption by policy makers post 911 was on the basis of security. Biometric passports emerged in response to US demands for a secure travel document for visa waiver countries following the attempted terrorist attack made by Richard Reid, a UK national (see Aus 2006, Bronk 2007). In public discourse, biometrics was represented as ‘100%’ secure: capable of making identity theft impossible (Times 2003, Pieri 2008, 17). This emphasis on security was also shown in the design of the NIS, where there was no indication of secondary systems (though, as Wills argues, the overall rationale for the NIS shifted considerably during its lifetime – see Wills 2008). For example, in the 2006 ‘Strategic Action Plan’ there is a list of the different identification services which the NIS was to provide (Home Office 2006, 11). Five different ‘levels’ of service were identified, based on the amount of security required: from a visual check of your resemblance to the photo printed on the card (the lowest) to a biometric check of your fingerprint against that present on the card (the highest). Beyond this fingerprint, there is nowhere else to go: if you fail that check, by implication, whatever transaction you were attempting to enact is over. Here, in other words, the system is biased entirely towards biometrics for security: there is no secondary system, no recourse for those who fail the check.

However, strikingly, whilst biometric technology has been successfully attached to two public identity documents in the UK (the ID card which has since been cancelled, and the ePassport which still exists), it is very rarely *used*. One of the few genuine implementations of the technology is at one of the new automatic border control gates which can be found in a few airports in the UK such as Gatwick, Stansted and Manchester (see Business Weekly 2009). These gates provide a test case: biometrics were built for security, is that how they are being used?

Speaking at a delegated legislation committee about the passage of new legislation surrounding the border control gates, Phil Woolas (Minister for Borders and Immigration) said the following:

> ‘I emphasise that use of the gates is entirely voluntary. They have two main benefits: they allow eligible users to enter the UK quickly and efficiently and reduce the number of low-risk passengers queuing up at manual immigration control allowing our UK Border Agency officials to focus staff resources on the higher-risk passengers at the primary checkpoint’ (House of Commons Seventh Delegated Legislation Committee 2010)

[5] Professor M. Angela Sasse, Head of Information Security Research at University College London, is an expert on human-centred approaches to security. She has conducted many usability and user acceptance studies of authentication mechanisms, including biometrics. She has also acted as an advisor to UK Parliament and the Identity & Passport Service over the National Identity Scheme. Interview was conducted with the author on the 25th of August, 2009.

Woolas, in other words, perceives two functions mainly relating to speed and efficiency: it is quicker for the passenger, and easier for the border guards. However, there remains a latent security justification: as the border guards have less passengers to check, they will be able to focus more on them. Therefore, whilst the technology is entirely voluntary, by not using it an individual is nevertheless considered by implication to be more high risk. How this focus materialises in practice is an open question. If the amount of time and the thoroughness of security check is genuinely related to the volume of passengers waiting, then this is an interesting demonstration of a relationship between security and efficiency in which security is not always the most important factor. However, most (admittedly anecdotal) evidence collected during research suggests that the security of the secondary passport check is no higher than that of an airport without the gate installed. It would therefore appear that the addition of biometrics to UK passport gates is, at least at the moment, serving solely a speed related function.

Why are these public biometric technologies, deployed at such expense, not being used for the security purposes for which they were envisioned? The lack of deployments in general, and the presence of these secondary systems where they are deployed, indicates that no-one currently trusts the biometrics to work 100% of the time, and no-one wants to pay the cost of a system that would perhaps be more secure yet generate a significant amount of mistakes every day. It is this lack of faith, which relates to the above discussion about the construction of success and failure rates, which is now contributing to the reconstruction of biometrics as tools for speed.

Again, the process described here poses problems for the idea of democratically controlling a technology. If it is difficult to define what a system will do prior to its construction, the very notion of "control" itself becomes extremely problematic. However, this is not to argue that technologies should never be allowed to shift functions. In the case of biometric passports, this shift actually appears to be quite positive. Instead of imposing a security tool which would place a burden on a small but significant percentage of the population, biometrics have developed into something voluntary and convenient for the user. One can debate, of course, whether this function justifies the expense of adding the technology to passports in the first place. Nevertheless, given that they had already been added, this development appears to be to the benefit of the scheme. Rather than arguing for more control of technology before deployment, therefore, this story seems to point to the need for technology to be controlled *after* it has been developed.

Conclusion

This paper has explored some of the processes by which knowledge about technologies is constructed. It has argued that the meaning of a technology is constructed alongside its physical manifestation, and has identified three areas where this has occurred in the case of biometrics in the UK: its construction as both a normal and exceptional technology; the debate over whether it is a success or failure; and the different possible functions which the technology can pursue. Throughout, it has remained faithful to the general ANT principle that action should leave a trace, and has tried to tackle big, nebulous questions such as how much faith people invest in biometrics, or whether they believe they are proportional, through reference to concrete proxies such as the strength of secondary systems, or the opinions of the ICO.

It has also remained objective towards biometrics, taking no particular stance on whether it works, or whether its use can be justified. It seems worth concluding, however, with a few more normative, practical points. Where should this study fit in to the broader struggle over surveillance and society?

The war on terrorism has coincided with the rise of the information society. The terrible events of 911 occurred at the beginning of the internet's second decade, just as policy makers were starting to consider new public interventions in the field of identity systems. This war, and the subsequent connection of security needs to public identity systems, has marked how we think about all sorts of identity management technologies, including biometrics. Rather than flexible, agile tools which allow people to take advantage of new services or perform on-line transactions, they have become imagined as invasive, intrusive databases, which impose onerous requirements on the person to update with their every movement. This security need, furthermore, has apparently stimulated a large scale public investment in a technology for which information is highly limited and where significant disagreement exists about what the technology does, how it works and what the costs are. In this sense, it is difficult to argue that biometrics in the UK have been democratically controlled.

In the case of the UK, however, it appears that biometrics, at least as a security tool, is in fact struggling to materialise. In this respect, it is interesting to note that whilst security concerns appear to allow the commencement of surveillance technologies such as biometrics, when it comes to their implementation the need for security systems to run efficiently and at low cost to those using them reasserts itself. In this respect, perhaps hearteningly, one can point to at least a partial control exerted by society over biometrics. The next few years could be crucial to the development of the technology: one only needs to look at the recent reverses suffered by internet voting to realise that the introduction of new technology is not inevitable, and promising new devices can be abandoned just as quickly as they are adopted if they fail on a large scale. The future of biometrics in the UK is in the balance.

It is too early to know how this future will turn out. Whatever the case, the consistent argument of this article has been that academic study needs to focus not only on understanding biometrics, but studying how other people come to understand them. In particular, the evidence gathered here points to a need for more high profile and transparent methods of evidence creation for the functioning of technologies like biometrics. Democracies need processes which lend legitimacy not only to decisions, but to the knowledge which forms the basis of decisions. The UK has significant expertise in the area: yet these experts are poorly represented in the public sphere. An impartial body charged with the creation of this evidence, with a strong media presence and a reputation for fairness, would be a significant asset in public debate over the management of surveillance technology.

While we continue to live in democratic societies, surveillance technologies will continue to be democratically controlled. This paper has tried to show the practical difficulties democracies face in realising this control, but also point to ways in which this challenge can be made easier. Information will never be perfect: yet it can be a lot better than it is. Proportionality can always be hard to define: but by empowering bodies who can tackle cases in their specificity this definition can become easier. Functions can shift: but this can be for the better or the worse, and the important thing will always be that society itself controls, to some extent, the change.

Acknowledgements

An earlier version of this paper was presented at 'A Global Surveillance Society?', the fourth Biannual Surveillance and Society/SSN conference, London, April 2010. Many thanks to all those who attended the panel "Biometrics" for their interesting critiques and suggestions. I would also like to acknowledge Antoine Vandemoortele, Christophe Lazaro, Claire Staath and one anonymous reviewer who provided very helpful comments and suggestions on various drafts of this paper, and Aaron Martin for providing me with many stimulating discussions and a host of references about the use of biometrics in the UK. Finally, many thanks to Professor Pascal Vennesson for his help, support and encouragement throughout all aspects of this research. All errors and omissions remain my own.

References

Aus, Jonathan. 2006. Decision Making Under Pressure: The Negotiation of the Biometric Passports Regulation in the Council. *Arena Working Paper* No. 11

BBC News. 2001. On the Record. Available from: http://www.bbc.co.uk/otr/intext/20010923_whole.html

BBC News. 2005. Id trials reveal scan problems. Available from: http://news.bbc.co.uk/2/hi/uk_news/politics/4580447.stm

Bijker, Wiebe. 1995. *Of Bicycles,Bakelites,andBulbs:Toward a Theory of Sociotechnical Change*. London: The MIT Press.

Bijker, Wiebe and John Law, eds. 1992. *Shaping Technology/Building Society*. London: The MIT Press.

Business Weekly. 2009. Stanstead Passengers urged to show their faces at hi-tech check-in gates. Available from: http://www.businessweekly.co.uk/2009051234912/travel-and-transport/stansted-passengers-urged-to-show-their-faces-at-hi-tech-check-in-gates.html

Buzan, Barry, Ole Waever and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner.

Callon, Michel. 1986. Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. In *Power, Action and Belief: A New Sociology of Knowledge?*, ed. John Law, 234-263. London: Routledge & Kegan Paul.

Campbell, Alastair. 2008. *The Blair Years*. London: Arrow Books.

Cole, Simon. 2001. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge: Harvard University Press.

Collins, Harry. 1981 'Stages in the Empirical Programme of Relativism', *Social Studies of Science* 11: 3-10

Constant, Edward. 1980. *The Origins of the Turbojet Revolution*. Baltimore: Johns Hopkins University Press .

Gooding, David, Trevor Pinch and Simon Schaffer, eds. 1989. *The Uses of Experiment*. Cambridge: Cambridge University Press.

Guardian, The. 2006. Fifth defeat for ID card scheme. Available from: http://www.guardian.co.uk/politics/2006/mar/28/immigrationpolicy.idcards

Haggerty, Kevin. 2009. 'Methodology as a Knife Fight: The Process, Politics and Paradox of Evaluating Surveillance'. In: *Critical Criminology*, Vol 17, 277-291.

Heath, William. 2005. Understanding the biometric trials: an expert explains. In: *The Ideal Government Blog*. Available from: http://idealgovernment.com/2005/06/understanding_the_biometric_trials_an_expert_explains/

Home Affairs Select Committee. 2004. Identity Cards: Fourth Report of Session 2003-2004. London: The Stationery Office

Home Office. 2002. *Entitlement Cards and Identity Fraud: A Consultation Paper*. London: The Home Office

Home Office. 2003. *Identity Cards: The Next Steps*. London: The Home Office.

Home Office. 2006. *Strategic Action Plan for the National Identity Scheme*. London: The Home Office.

House of Commons Select Committee on Science and Technology. 2006. *Identity Card Technologies: Scientific Advice, Risk and Evidence (Report HC 1032)*. London: The Stationery Office

Hughes, Thomas P. 1986. The Seamless Web: Technology, Science, Etcetera, Etcetera . In: *Social Studies of Science* 16 no.2: 281-292

Infosecurity. 2009. Biometrics 2009: Schools are spearheading the use of biometrics. Available from: http://www.infosecurity-magazine.com/view/4844/biometrics-2009-schools-are-spearheading-the-use-of-biometrics-/

Information Commissioner's Office. 2007. The use of biometrics in schools. Available from: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view.pdf

Jasanoff, Sheila. 2005. *Designs on Nature*. Princeton: Princeton University Press

Kaluszynski, Martine. 2001. 'Republican Identity: Bertillonage as a Government Technique. In: *Documenting Individual Identity*, eds. Jane Caplan and John Torpey. 123-138. Princeton: Princeton University Press.

Latour, Bruno. 1988. *The Pasteurization of France.* Trans. Alan Sheridan and John Law. Cambridge: Harvard University Press.

Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Latour, Bruno and Steve Woolgar. 1979. *Laboratory Life: The Construction of Scientific Facts*. Sage: Beverly Hills.

MacKenzie, Donald. 1989. From Kwajalein to Armageddon? Testing and the social construction of missile accuracy. In: *The Uses of Experiment*, eds. David Gooding, Trevor Pinch and Simon Schaffer. 409-436. Cambridge: Cambridge University Press.

MacKenzie, Donald. 1990. *Inventing Accuracy*. London: The MIT Press.

No2ID. Frequently Asked Questions on Identity Cards. Available from: http://www.no2id.net/IDSchemes/FAQ/

Oudshoorn, Nelly and Trevor Pinch, eds. 2003. *How Users Matter. The Co-construction of Users and Technology*. Massachusetts: MIT Press.

Pieri, Elisa. 2009. *ID cards: A snapshot of the debate in the UK Press*. Manchester: ESRC National Centre for e-Social Science.

Privacy International. 2004. *Mistaken Identity; Exploring the Relationship between National Identity Cards and the prevention of Terrorism*. London: Privacy International.

Russell, Stewart. 1986. The Social Construction of Artifacts: A Response to Pinch and Bijker. *Social Studies of Science* 16, no.2: 331-346.

Sankar, Pamela. 2001. DNA-Typing: Galton's Eugenic Dream Realized? In: *Documenting Individual Identity*, eds. Jane Caplan and John Torpey. 273-290. Princeton: Princeton University Press.

Sengoopta, Chandak. 2003. *Imprint of the Raj: How fingerprinting was born in colonial India*. Oxford: MacMillan.

Telegraph, The. 2005a. Met chief says ID cards must be near perfect. Available from: http://www.telegraph.co.uk/news/uknews/1492124/Met-chief-says-ID-cards-must-be-near-perfect.html

Telegraph, The. 2005b. Chief scientist to put ID biometrics under the microscope. Available from: http://www.telegraph.co.uk/news/uknews/1501503/Chief-scientist-to-put-ID-biometrics-under-the-microscope.html

Thompson, Scott. 2008. 'Separating the Sheep from the Goats: The United Kingdom's National Registration Program and social sorting in the pre-electronic era'. In: Bennett, Colin and David Lyon, eds, *Playing the Identity Card*. London: Routledge

Times, The. 2003. Technobabble. Available from: http://www.timesonline.co.uk/tol/life_and_style/article1019239.ece

Times, The. 2004. ID cards defned the ultimate civil liberty. Available from: http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article404360.ece

United Kingdom Passport Service. 2005. *Biometrics Enrolment Trial Report*. London: UKPS

Vincenti, Walter G. 1990. *What Engineers Know and How they Know It*. Baltimore: Johns Hopkins University Press.

Whitley, Edgar A. and Gus Hosein. 2009. *Global Challenges for Identity Policies*. London: Palgrave Macmillan

Wills, David. 2008. 'The United Kingdom identity card scheme: shifting motivations, static technologies'. In: Bennett, Colin and David Lyon, eds, *Playing the Identity Card*. London: Routledge

Winner, Langdon. 1993. Upon Opening the Black Box and Finding it Empty: Social Constructivism and the Philosophy of Technology. *Science, Technology and Human Values* 18, no.2: 362-378.