

The Face Of The Future

Biometric surveillance and progress

RANA DASGUPTA



Perhaps a good test of the effectiveness of a democracy might be whether or not it permitted the populace to say “No” to any more progress: to declare that a particular technology had been taken far enough, and should not be taken further; that new kinds of change were likely to make society worse rather than better, and should cease.

If we think that most democracies might fail such a test it is probably because we feel that progress’ ongoing process of destruction and recreation is more fundamental to modern hi-tech democracies than plebiscites. For the united middle classes of the world it is difficult to conceive of time itself outside of the notion of a movement from naivety (past) to technology (present, future). The word ‘progress’ has become pretty much detached from any kind of ethical vision, and as it becomes an inexorable drive of pure power, profit and technology this seems only to consolidate its position as something fundamental to the mechanics of the universe.

But 'progress' is not predefined. The unfolding of the future is a confused process, full of conflict, and public opinion is not so mute in this as it might appear. New social forms, new technologies, new processes of control must all legitimise themselves under the rubric of 'progress' and there are limits to the flexibility of the category. The genetically modified food industry, while presenting its new products as merely the next stage in an age-old history of selection and breeding ('progress'), has still not managed to achieve this legitimacy in much of the world. Food seems to be one domain where people wish their connection to the natural not to be broken, and though the concept of 'the natural' may have been stretched very far, genetically modified foods still seem to lie outside it for many people. The industry has spawned lobby groups all over the world, and 'offshore' PR bodies aimed at presenting an independent, unruffled picture of more food and happy farmers, but publics outside the US, already panicked by (sometimes unrelated) natural disasters such as BSE or foot-and-mouth disease have remained largely unreceptive. The equation more technology=better world does not always work.

Biometrics and progress

Another area where this fight for legitimacy is going on is in the area of biometric systems of identification and authentication. The technologies exist, their usefulness in what Deleuze would call a 'control' society is clear, but the public has just taken a long time to understand what's good for it. In fact the scanning of fingerprints, irises or DNA as a prerequisite for access to buildings or information has long been a staple part of the nightmare of Hollywood sci-fi fantasies. In such scenarios the private realm has usually been completely eradicated, and in films like *Gattaca* our experience of this universe is via the tortured interiority of an interloper – whose pariah status allows him to retain the humanity that everyone else has lost – whose only remaining privacy is the secret terror that he will be discovered. (As we'll see, in the marketing of biometric systems, such interlopers are always someone else). It may actually be that such science fiction dystopias do a lot to 'prepare' us for the unpleasant futures they present by making natural the progression that results in increasing levels of technological control in society; but still the fear of being continually scanned and tracked is one that companies who are betting their future on more scanning and tracking have somehow to 'deal with'. They too have hired PR firms to help insert their products into the benign sweep of progress and set up an industry association in Washington, DC, the International Biometric Industry Association (IBIA) that lobbies for its interests.

But this industry has had a happier time recently than the biotech giants. Current affairs have intervened to give a massive boost to the PR campaign, and since 11 September 2001 biometrics executives have become the good guys, avuncular in their sympathy for the afflicted, grim in their determination to find a solution, and fêted in all the media from CNN to the *Washington Post*. To quote a *Business Week* report from 2 October 2001 on the post-September 11 market catastrophes that were crushing most other technology firms, "Biometric companies, which sell devices that authenticate individuals by scanning unique identifiers such as fingerprints or retinas, are... expected to do well. The uphill public relations battle that before Sept. 11 afflicted such outfits as Visionics (VSNX),

which makes controversial facial-recognition software, is easing. Visionics stock has skyrocketed nearly 150% since Sept. 11”.

The boost to the performance of these companies has since been much more dramatic even than this. Visionics’ stock increased from a high of US\$ 4.50 on September 10 to US\$ 16.89 six weeks later. Competitor Imagis Technologies Inc. saw its value increase nearly five times over the same period. Such dramatic rises were fed by veiled references to imminent mega deals, uttered with a mixture of barely contained glee and the dignified confidentiality of the newly elect, as in this press release from Imagis (issued on September 14 to explain to anyone who was wondering why they were suddenly doing so well), “Imagis Technologies Inc., (‘Imagis’) reports that the substantial increase in the company’s stock price is due mostly to Imagis biometric facial recognition technology. The tragedy that took place last week has turned attention to those companies that have the technology to assist in airport security, customs and immigration, law enforcement and criminal justice. In the past, Imagis has made a number of technology presentations and demonstrations of its software capabilities to major system integrators and government agencies in the United States and in other countries worldwide. Over the past week, many of these organisations have contacted the company to assist in the development of identification, airport and security system installations using its biometric facial recognition technology, ID-2000”.

Analysts who had hitherto been wary of overvaluing a small and unpopular industry have been frenetically revising their calculations. While most agreed before September 11 that the industry would not be worth half a billion dollars before around 2006, an analyst from Morgan Keegan & Co. recently predicted a ten-fold growth in total revenue over the next two years to around US\$ 2 billion by 2004. As the *Washington Post* reported on 1 November 2001 in a fascinatingly eloquent statement on public, progress and technology, “Industry analysts said the attacks probably accelerated by years the public’s adoption of face recognition and other biometric systems that rely on immutable human features”.

In this new climate of warm handshakes and non-stop ringing telephones these companies have scrambled to cut deals that will consolidate their positions. On December 7, Visionics issued a press release declaring a partnership with “ARINC Incorporated, the leader in mission-critical communications and information-processing systems for the aviation industry”, a partnership in which ARINC will sell Visionics’ Facelt® system as an integrated part of all its other airport systems. Michael V. Picco, staff vice-president of ARINC Airport Systems, stated, “Aviation security is a major area of focus for our systems integration efforts. We are committed to providing the best solutions to the myriad of security challenges that the airlines and airports face today. A key component of these solutions is facial recognition, and our alliance with Visionics gives us access not only to the best-of-breed biometric technology in this area, but also to a scalable platform on which to deliver it. The alliance will focus on meeting the broad security needs of the airline industry, a market sector in which ARINC is well established. ARINC is owned by a consortium of leading airlines, aircraft makers and operators based in the United States and around the world, including United Airlines, American Airlines, Boeing, FedEx, British Airways, Lufthansa and Raytheon”.

As these deals congeal, the various companies are fighting a cut-throat battle over

standards and technologies, and everyone is flaunting their own blue-chip credentials. The senior executives in these companies have backgrounds in the top universities, the top corporations and the top intelligence agencies. Dr. Joseph Atick, the CEO and co-founder of Visionics Corporation, who humbly advertises himself as “a renowned visionary and business strategist” has directed the Computational Neuroscience Laboratory at Rockefeller University and the Neural Cybernetics Group at the Institute for Advanced Study in Princeton. The CEO of another facial recognition company, Viisage, spent 20 years with Digital Equipment Corporation during which he was responsible for selling their products to the US Federal Government and the aerospace, electronics and manufacturing industries. The list of his awards from Vietnam is impressive. The Chairman of Imagis is Oliver “Buck” Revell who was Associate Deputy Director of the FBI. The list goes on. A nexus of people with significant intellectual and enormous political and industrial power have the courage and the capital to realise grand visions of technological order. Joseph Atick, for instance, envisions his technology being used to construct a “national shield” of face-recognition systems linked to government databases filled with images of known terrorists (*Washington Post*, 1 November 2001). For sublime technocratic missions like this, public opposition is a real irritation.

A new imagination

Clearly then, ignorant and even rash public opposition to such systems needs to be crushed immediately so that policy can proceed rationally and responsibly. As the IBIA's mission statement puts it, “[The growth of the industry] could be severely constricted... by misinformation as well as a lack of public awareness about biometrics. In particular, concerns about privacy can lead to ill-informed regulations that unreasonably restrict the use of biometrics on identity documents, in financial commerce, benefits administration, and other important consumer applications. In the absence of common and clearly articulated industry positions on issues such as safety, privacy, and standards, governments will react rashly to uninformed and even unfounded assertions about the function and use of biometric technology”.

So as the products of these companies become an accepted part of the changes that are called progress, as they become banal rather than Orwellian – their technologies ‘just’ technology and their businesses ‘just’ business – they must also spawn new social visions and new aesthetics that give a rationale to the new directions. Anxious visions of ubiquitous threats, of once familiar places turned eerie, of people guilty and craven until verified otherwise. Aesthetics that privilege the deep, pure vision of technology over the inadequate corrupt realm of the human.

The companies who make facial recognition systems, whose purpose is to detect the presence of suspicious people in public places, have the most baroque imaginations of them all. The page devoted to Imagis' airport security systems says “Do you really know who's coming through your airport?” and has a picture of a middle-aged white man whose evil smirk and slightly-too-open shirt belie the openness with which he exhibits his passport. A few minutes surfing through the pages and pages of evil faces makes the need for protection provided by products like Trespass-ID seem completely natural: “Trespass-ID is a

biometric software application designed specifically for security professionals who need a better way to identify and track undesirables, their associates, and specific behaviours, before they commit crimes and do damage”.

But even fingerprint or iris scanning companies, who require the cooperation of an individual in order to scan his or her data and therefore have to create a friendlier image, must fundamentally stoke fear to justify their existence. A representative from EDS interviewed by CNN at the Comdex technology show on November 15 explained that the company's palm reading device was “meant to ensure that the person sitting next to you on the plane is who they say they are”. DigitalPersona, who provide a desktop fingerprint scanning device to allow Internet users to identify themselves to distant databases as they surf, hints more gently at the danger, “DigitalPersona provides its customers with a convenient and secure means of digital identification that ensures convenient interaction with digital systems, and a safe journey through the wonders of Cyberspace”.

At the same time, these companies are aware that most people's first encounter with their products will be an anxious one, and they have to appeal to that other pillar of ‘progress’ – customer service and convenience – to plug their products over those of their competitors. Scanning devices are presented as if they were a new kind of friend; as DigitalPersona says, “Interactive digital systems present us with new, life-enhancing opportunities and experiences, and are becoming integral to our personal and professional lives. In order to make use of these product advancements we must be able to identify ourselves to them, and doing so must be as easy as reaching out to shake a hand”.

“We never forget a face”, declares Imagis' web site about its face recognition systems, in a phrase that is more warped than perhaps it intends. In a more slick formulation worthy of the industry dandy that he is, Joseph Atick says, “Facial recognition technology automates what humans have done since the beginning of time – recognise one another face-to-face”. The CEO of DigitalPersona, Fabbio Right, echoes this futuristic nostalgia, “Over the course of hundreds of years, signing a piece of paper has become part of our lifestyles. We are trying to accomplish the same thing with biometrics. Little by little, people will get used to it”.

What is interesting about this elegant but rather perverse humanisation of the technology is that it corresponds to a simultaneous technologisation of the human being, a vision of the individual in which his or her deepest truth had always been comprised of 1s and 0s, and it was not until the arrival of technologies that could detect these inner codes that human beings could truly be known. Thus the constant graphics throughout the marketing literature of these companies in which human beings are stripped of all inessentials and covered with 1s and 0s seem to represent their deepest essence. As they bask in the gaze of the recognition technology it seems to be a moment of ecstasy, of apotheosis of the self. Data basing human beings is not about intruding upon the lives of individuals but knowing them as they always wanted to be known.

The transformation of the everyday

The spread of such technologies will not be unobtrusive. Face recognition techniques, for instance, currently require the camera to capture a full-on image of a face in order to be

able to map it, and will therefore require either a very large number of cameras to guarantee that every individual (for instance in an airport) is caught thus by one of them, or the presence of roving cameramen with a device such as Xybernaut's "crowd-scanning head-gear", which fits over one eye and allows the user to scan faces by looking at them while it compares the scanned images to those stored in a remote database via a wireless connection. But there is no doubt that there is significantly greater investment now in biometrics than was the case before September 11, and that these technologies and the social imagination that makes them reasonable will infiltrate the everyday to an increasing extent. A bill stands waiting for passage in the German Bundestag that would insist on biometric data being stored in German ID cards and passports. DigitalPersona's products are fully compatible with Microsoft's new XP platform so that companies can already require users to identify themselves with their fingerprint rather than with a password. The logic will become self-evident – how could one have imagined that a PIN number was enough to ensure the security of an ATM card? – ATM machines need face recognition too. And then, suddenly – "NEW! The PINless ATM card that goes entirely by face recognition. Now all you need is you. We don't treat our customers as a number – we never forget a face!" It won't be possible anymore to give your ATM card to someone else to get money out for you.

As biometric systems become part of the happy paraphernalia of travel or the caring solidity of banks they will indeed become banal. The Visionics press release quoted earlier also mentions, for instance, that the company's systems are already being presented as part of a drive towards convenience, "International Air Transport Association (IATA) special interest group on simplifying passenger travel – called SPT... SPT is a worldwide, forward-looking initiative consisting of airlines, airports, government authorities, system integrators and vendors who recognise that today's airports are not built to handle the massive throughput of travellers. SPT has outlined the vision of a future system that takes into account technological advances that can simplify passenger travel and make it more secure. As such, facial recognition is poised to play a major role, particularly since it has already been endorsed by the International Civil Aviation Organisation (ICAO) as the most suitable biometric for air travel".

As they sprout rapidly in such areas as airports, it will be important for these rather intimidating systems to explain their sudden presence. The companies will need to show the public high-profile examples of what dangers can be averted with a Trespass-ID system in place, and much zealous use will surely result in some dastardly individuals going where they deserve. As similar products become available for home security too, the public will also to some extent buy in to the notion that only biometrics offers true identification and authentication. Institutions of control will come to rely on the new kinds of data that will suddenly be available and the idea of removing all these expensive systems – of saying "No" to all this progress – will become unthinkable.

But these technologies will have a significant effect on interiority. By allowing your very face to be converted into a digital code that can be checked at any moment without the need for any consenting action from you (such as the swipe of a credit card), they alter the imaginary realm considerably. The possibility of being known at any point, of your identity being continually checked – in banks, shopping malls, airports etc. – against

everything else that is known about you will seem like a massive escalation in the observation matrix from the more occasional 'checking-in' we currently do with each passport check or ATM withdrawal.

Surveillance is usually blind to what is prescribed as 'normal' behaviour. It triggers a reaction when it picks up an event that is considered abnormal for some reason or another. The effect on behaviour is thus to whittle away at the edges of the self and impose an anxious homogeneity. It will, as in *Gattaca*, lead to a more paranoid self in which the public realm will be a hostile and tiring place where you wonder constantly if you're looking innocent.

What are biometric systems?

Biometric systems are designed to verify the identity of a person by checking some unique biological characteristic against a database. They are used in two ways. Authentication: checking that this person is who they say they are – or what the industry calls 'one-to-one' matching. This would be used for border controls, access to physical environments such as offices, and access to web sites, bank account details etc – i.e. for any situation where currently a password or document proof of identity would be the norm.



Identification: finding out who a person is by checking them against a large number of stored identities – or 'one-to-many' matching. This is used for identifying suspicious people in public spaces such as airports, shopping malls etc. Different systems use different biological traits as their basis. These include: fingerprint, DNA, voice, face shape, palm print and the pattern of the iris. All of these provide a reliability of close to 100%, though there is much industry wrangling over which the most reliable is.

Not all techniques are useful for all environments, however. Identifying people in a crowd necessarily relies on facial recognition, which can be carried out at a distance. Facial recognition works (in the case of Visionics' system) by mapping some 80 facial 'landmarks' and is supposedly unaffected by superficial alterations such as facial hair or glasses. It can be carried out by cameras that take several images a second, convert those images to a facial code and check that code against a database. Joseph Atick, CEO of Visionics, claims that images are not stored if there is no suspicious history in the database corresponding to that person. If you haven't done anything, you haven't got anything to worry about.

For authentication it is more common to get people to scan their fingerprints or irises, which can be captured more easily.

Advocates of biometric systems say that they offer cheap and effective protection against such threats as credit card fraud or impersonation on the Internet, and against crime and terrorist activities.