The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies

Julian Ashbourn

Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission

January 2005

Legal notice
Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

Disclaimer
The author of this report is solely responsible for the content, style, language and editing. The views expressed do not necessarily reflect those of the European Commission.

Preface

In June 2004, the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs of the European Parliament (the LIBE Committee) asked the JRC to carry out a study on the future impact of biometric technologies. The report *Biometrics at the Frontiers: Assessing the Impact on Society* (EUR: 21585)[1] is the result of this request. The work was carried out by staff from the IPTS ICT Unit, in collaboration with a number of external experts.

Four experts were asked to contribute to the study, expressing their views on the technical, legal, social and economic implications of biometrics. They were respectively Professor Bernadette Dorizzi of the *Institut National des Télécommunications* (INT), FR; Professor Paul de Hert, of the faculty of Law, University of Leiden; Julian Ashbourn, chairman of the International Biometric Foundation and creator of the AVANTI non-profit on-line biometric resource (http://www.avanti.1to1.org); and Jonathan Cave, Senior Lecturer at the Department of Economics, University of Warwick, UK, and Project Leader at RAND Europe.

The above mentioned report *Biometrics at the Frontiers: Assessing the Impact on Society* contains the summarised contributions from these experts (in Chapter 3). More extended versions of their contributions are published on the IPTS website as background studies.

The present document is the extended version from Julian Ashbourn on *The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies.*

Available at: http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm

[1] Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodríguez, C., Ulbrich, M., Cabrera, M., Clements, B., Beslay, L., & van Bavel, R. (2005) Biometrics at the Frontiers: Assessing the Impact on Society. Study for the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), IPTS, Sevilla, February 2005.
Available at: http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm

The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies

Julian Ashbourn

Contents

1. Introduction

Technology is a tool which may be developed and used intelligently or unintelligently, ethically or unethically, for the common good or against the common good. When we introduce new technologies which will affect the lives of many millions of individuals, we must bear such realities in mind and strive to do so in a responsible manner. Biometrics and related enabling technologies are a case in point. It is not enough to make assumptions about biometrics and their role in society. We must dig deeper and understand – really understand, the implications of introducing such technologies on a wide scale within the public sector. Not just the immediate implications, but the longer term societal implications. Make no mistake, we are introducing a fundamental change in the trust model between citizen and state which will affect ourselves, our children and future generations. Concepts such as anonymity and personal privacy are being challenged while the traditional concept of being considered innocent until proven guilty, one of the cornerstones of free society, is being dismissed in relation to everyday transactions such as border crossing. Such an undertaking carries a heavy burden of responsibility. If we do it poorly, we shall not only fail to achieve any significant benefits from a security perspective, but we shall negatively impact the quality of life for millions of people and erode public confidence accordingly. This is not a matter of scare-mongering or trying to attach a negative connotation to current political aspirations in this area, but simply drawing attention to a very real possibility. A possibility accentuated by the speed with which such aspirations are being pursued. If, on the other hand, we do things well, then there are certainly benefits to be realised from the intelligent and responsible use of biometrics and related technologies.

To date, much of the discussion in this context has been of a technical nature. We have concerned ourselves with the technicalities of biometric template formats, portable storage such as embedded chips and the practical considerations of tokens such as chip cards and smart passports. We have also expended much energy on discussions around theoretical performance and have spent years discussing suitable standards. Qualified discussion around the longer term societal implications has however been conspicuous mostly by its absence. This paper will go some way to restoring the balance, although it is stressed that more research in this area would be desirable, as would true national, European and international coordination. In order to properly understand and discuss such matters, we must first place this technology in context. The following section therefore offers a brief introduction to biometrics from a societal and historical perspective, together with an overview of the currently popular techniques. This will equip the reader with a point of reference in relation to concepts and ideas discussed subsequently.

2. Background

Biometric identity verification may be undertaken by matching a live instance of the biometric with a previously stored sample, or may be undertaken off-line by matching two instances of stored samples. The former process may be undertaken in real time for transactional purposes and requires the presence of the individual in question, the latter process may be undertaken entirely by third parties, as would be the case for example in law enforcement when matching sets of fingerprints.

Contrary to popular belief, the concept of using a biometric for identity verification purposes is not new and dates back certainly to ancient Egyptian times, if not before (Babylonian kings supposedly used impressions of the hand in clay for identity verification purposes for example). Since then there has been a general fascination with aligning physiological traits with both identity and character, with much activity at the turn of the 19th century. Around that time, Franz Joseph Gall in Germany, undertook much work in the area of phrenology, hoping to align cranial features with character traits. This concept was fascinating to many, including an Italian named Cesare Lombroso who further aligned phrenology with criminal behaviour, setting off a train of thought that was to be particularly far reaching. The science of anthropometry emerged, which covered the measurement of various anatomical traits, including limb circumference and weight in order to align with identity and character. The Belgian Adolphe Quetelet published a popular treatise on the subject in 1871 entitled, L'Anthropometrie ou Mesure des Differentes Facultes de L'Homme, and creating further interest in the overall concept. In Paris, the head of the identification service at the Paris police headquarters, Alphonse Bertillon, picked up the thread and introduced the concept of judiciary anthropometry, using anatomical measurements in order to identify criminals. This idea quickly gained ground with others adopting the principle, even though this was not at the time a well proven technique. Clearly the desire for something along these lines was very real among government agencies, a situation which is somewhat echoed today with respect to biometrics.

In 1823, the Czech, Jan Evangelista Purkinje was studying sweat glands when he came to the conclusion that the pattern of ridges at the finger tips seemed to be unique. This discovery, somewhat secondary to Purkinje's objectives, proved to have far reaching consequences, leading to a system of identifying criminals that is universally accepted today. The process of taking fingerprints as ink patterns is known as dactyloscopy and was first practiced by an Argentinian police officer by the name of Juan Vucetich who, in 1888, published a treatise on comparative dactyloscopy. In the 1890s Englishman Francis Galton, a cousin of Charles Darwin, was engaged in various studies in human sciences including twins and the classification of fingerprints. This work lead to the creation of the Galton-Henry fingerprint system which was introduced in Scotland Yard in June 1900. From that point onwards, the association of fingerprints with criminology was firmly established.

As we have illustrated above, the idea of using anatomical traits in relation to identity verification is not new and has been fascinating people for a very long time. A significant milestone was the marrying of this concept with the power of electronics, which first took root in the 1960s with various experiments being undertaken in this context. This raised the possibility of automated checks against a stored reference, an early example being the work on hand geometry initiated by the Miller brothers in America. Hand geometry was further developed as a viable biometric technique when parallel developments in electronic components allowed for a considerably more compact device to be designed and manufactured at reasonable cost. By the late 1980s there were several variations on automated biometric identity verification devices available, using techniques such as fingerprints, hand geometry and voice verification. Following on from those early devices, there has been a continual refinement in both the physical capture devices and the matching algorithms used, leading to the current situation where there are a plethora of readily available, relatively low cost biometric devices on the market. Fingerprint readers in particular are available from a wide number of sources as a commodity IT component, and are additionally integrated into a variety of host devices such as notebook computers, keyboards, PDAs and even mobile phones. As more devices become manufactured in the far east, the cost of biometric devices will become insignificant compared to overall programme costs. This will, in some respects, make it easier to integrate biometric functionality into host applications, although much will depend on the scope and scale of the application in question.

There are also a variety of biometric techniques, with new ideas continuing to surface in this area as well as ideas around using existing techniques in different ways (multi-modal biometrics for example). The currently popular techniques may be summarised with respect to their use, acceptance and impact as follows;

Fingerprints

Of obvious interest to the law enforcement community, fingerprints offer a well established technique where the base data is also well understood. Fingerprints may be matched by the comparison of the position of minutiae points or by a more general pattern matching approach. Fingerprint capture devices tend to be based upon either optical readers or capacitive based chips. This variation of both fundamental matching principle and capture mechanism provides for an interesting variety of devices, although does raise questions around true interoperability.

Hand geometry

As previously indicated, hand geometry is one of the longer running biometric techniques and there are a large number of devices in regular operation around the world. Most of these devices emanate from a single manufacturer (Recognition Systems – now part of the Ingersoll Rand group) who has accomplished a great deal in refining hand geometry into a workable and reliable methodology which lends itself well to physical access control applications.

Voice verification

A technique which would appear to have good promise, although to date it has been somewhat hampered by the vagaries of speech transmission systems, available low cost transducers and of course acoustics in an operational sense. Never-the-less there has been some good work undertaken in this area and it is a technique which may enjoy a resurgence of interest as we move along.

Retina scanning

The original retina scan biometric product offered good levels of accuracy at a time when other techniques were still developing. It was therefore adopted in various military applications where the cost of the technology was less of an obstacle to implementation and user preferences were not such an issue. In more recent times retinal scanning as a technique has failed to capture the interest of users and the technique has declined in popularity.

Iris recognition

Working on completely different principles from retinal scanning, iris recognition is far more user friendly and offers very high accuracy. Furthermore, iris scanning has been adopted under license by certain high profile electronics companies who are able to develop good quality, interesting products and have existing marketing options for their distribution.

Facial recognition

While early facial recognition products suffered from over-statement of their capabilities coupled to a generally unexciting performance, intervening years have seen a steady development of the technique to a point where performance is perfectly acceptable for a broad range of applications. This trend of evolvement continues with 3D variants and the addition of supplementary techniques such as surface texture analysis making facial recognition a viable biometric technique.

Vein patterns

Vein pattern recognition has in fact been around for some time but has perhaps not captured the imagination in the same manner as other techniques. The principle is that the vein patterns in the back of the hand and wrist are unique and may be clearly distinguished under certain lighting conditions, providing a usable identifier. There have been various products surface over the years and there is currently a slight resurgence of interest in this technique.

Signature verification

An obvious technique from some perspectives, signature verification has the perceived benefit of replicating a familiar process, that of signing one’s name. In theory it would seem well matched to applications where the signature is currently required as part of a transaction, as well as applications where visual information plays a large part, such as document control. In practice, although there have been some very interesting signature verification products, the technique has as yet failed to have a significant impact in the world of biometrics.

Keystroke dynamics

There was considerable interest in this technique for a while from the IT security area. The concept being that individual patterns are readily discernable when using a keyboard. In spite of considerable research and refinement, keystroke dynamics has not been used on a wide scale and currently languishes in the backwater of biometrics.

Gait recognition

This technique aims to recognise individuals by their distinctive gait, providing the promise of identity verification from a distance. There has been some good research undertaken into this area with demonstrations which suggest the technique has some merit. However, this has not yet been developed to the same level as other biometrics.

DNA analysis

The possibility of DNA being used as an operational biometric has often been discussed and explored. Certainly, such an approach would seem to offer high accuracy in terms of matching DNA samples, however, at present the analysis required in order to reach a positive or negative matching decision cannot be undertaken in real time, rendering such a technique impractical for the operational, i.e., real time transactional use of biometrics. It is therefore currently considered a technique better suited to traditional forensic applications. With regards to accuracy, there is a popular misconception that a DNA match is absolute. In fact, this is not necessarily the case and it is felt that more research would be needed before DNA represents a practical biometric for automated identity verification purposes. Whether this changes in the future, we shall have to see.

Other techniques

There have been various other techniques developed from time to time, some of which have been developed into prototypes and displayed at conferences and exhibitions around the world. However, the biometrics mentioned above are currently considered the most popular and usable at this time. There is also interest in multi-modal biometrics where two or more techniques, or variations on the same technique, may be utilised in order to enhance the accuracy or convenience of the overall process. There are arguments both for and against such an approach, of which we shall no doubt hear much more as time progresses.

It may be inferred from the above that the science of biometrics is well established with a variety of fundamental techniques and an even larger variety of readily available products and associated vendors. This is certainly the case and we are long past the point at which biometrics should be considered a new or emerging technology. However, the uptake of biometric identity verification techniques among mainstream applications has hitherto been relatively slow, with the biometrics industry remaining rather fragmented and slow to develop compared to other branches of electronics. The renewed interest in biometrics from a government perspective is set to change all this, with the introduction of several wide scale applications within the public domain. However, it is important to understand the real value of a biometric in this context and not to jump to conclusions based upon marketing propaganda. There is a great deal to understand in relation to wide scale applications, only a certain proportion of which is associated directly with technology.

3. The Public Sector Perspective

There has been an interest in using biometric technology for public sector applications since the early 1990s with, for example, trial systems for benefit payments and automated border control appearing in 1993. However, the events of September 2001 brought new impetus to governmental thinking in this context. The spectre of international terrorism was raised higher in the public perception and it was politically appropriate to be seen to be combating this societal ill. Personal identity verification and border control in particular have received the attention of government agencies throughout the world. One might question however the assumption that someone wishing to commit a terrorist act needs to cross a border in order to do so. This is clearly not the case. Similarly, it by no means follows that such an individual has an existing criminal record. The claim that stringent border controls currently being implemented will deter terrorists and make the world a safer place needs therefore to be qualified.

Of course, the current focus on terrorism, provides the opportunity for government agencies to implement more stringent control over citizens via national identity schemes and border control programs, for a variety of reasons which have little to do with terrorism. Herein lies an important issue – the blurring of citizen entitlement (including the entitlement to cross borders and access public services) with law enforcement. Many would argue that the two should be kept separate. On the one hand, we are dealing with mostly law abiding citizens who are simply wishing to access a service. On the other hand we are dealing with the criminal fraternity. Why should a law abiding citizen be treated like a criminal? This is a question which will probably be raised repeatedly as the media and general public start to understand what is really happening behind the scenes with border control, national ID and related schemes, especially with regard to the sharing of data across agencies and countries. A citizen is not a criminal because they wish to access a public service to which they are entitled, or cross a geographic border which they may legitimately cross. It is important to acknowledge and protect this premise, if we are not to suffer from dangerous levels of function creep.

With regard to data protection and privacy, border control procedures currently being operated between the European Union, the Americas and elsewhere, cut across almost every principle of existing acts. Data of a very personal nature is shared without the individuals permission and often without their knowledge. Furthermore, it is by no means clear what actually happens to this data, how long it is stored for and who has access to it throughout this period. This state of affairs is about to become more extreme as governments start profiling individuals and making assumptions based upon data such as family name, ethnicity, or travel history which could result in discrimination or denial of service based upon this information. We must therefore either acknowledge that there is effectively no such thing as data protection and privacy when dealing with government agencies, or, re-write the various acts in order to expressly exclude certain government functions from their provision. Many such acts already have a clause which provides exemption in matters of national security – another reason why the aforementioned distinction between the provision of public services and law enforcement must be made clear. If we are not absolutely clear on these points, we run the risk of eroding public confidence in governments ability to protect personal information. Recent surveys across a number of areas show a growing distrust of government by ordinary citizens. This is a worrying trend as it potentially provides a breeding ground for extremist views to develop, as all history shows us. It follows then, that we must be extremely careful when introducing technologies into the public sector which may be viewed as ‘big brother’ enablers. Adding a biometric identity check to everyday transactions may, depending upon how it is orchestrated, promote just such a view. There are undoubtedly some logical applications where the introduction of a biometric would be generally perceived as being for the common good, providing there is clear and full information given as to the details of implementation. This is a factor which, it must be said, to date has not been handled particularly well, both within and beyond the European Union. As we progress into the implementation of current aspirations, there is a risk of alienating responsible citizens unless a policy of honest and open discussion is adopted, together with the provision of full and detailed information as to the workings of individual schemes and precisely why they are being considered. The importance of this point cannot be overstated.

It is becoming clear to the majority that government agencies in general are inclined to take advantage of the perceived terrorist threat in order to introduce a variety of schemes under the general banner of ‘security’ whose real agenda is quite different. The writer is fully aware that he will not be thanked for making this point, but it is a point which *must* be made. The wide scale introduction of biometrics to public sector applications and activities represents a very significant societal change. If we embark upon this journey under a cloud of deception, then that cloud will follow us for a very long time. The irony is that many of these ‘other’ applications are probably quite justified and, if properly explained, would no doubt generally receive widespread public support – provided they are designed and implemented in an intelligent, ethical and responsible manner. Unfortunately, not all of the current aspirations reflect this ideal, as many have been rushed into with an inadequate understanding of the attendant issues. There is scope then, to develop some solid guidelines, recommendations and even legal requirements in order to support the introduction of these technologies in a socially acceptable manner. This is surely where the political focus of the European Union should currently rest.

4. The Reality of Large Scale Applications

There is a world of difference between a carefully orchestrated technology trial and a full blown large scale application which may require orchestration by several entities. Furthermore, these differences are not just of a technical nature, but require careful configuration from a process and ongoing management perspective. The success of a wide scale application, which may involve several agencies, including perhaps those from other administrations, will be measured partly by its acceptability from a societal perspective.

Let us first consider the technical perspective. There is no such thing as a biometric system. A biometric identity verification check is simply a defined function within a broader process. That process may be the provision of social services, a border crossing or some other transaction. The system supporting that transaction may be self contained or may need to reference other systems. Similarly the underlying infrastructure may be within the control of the administrating agency, or may not be. The realised ‘performance’ of the biometric identity verification check within that transaction will be a sum of all the components involved, including the biometric capture and matching process, any related database access activity, communications, system processing and, an often overlooked item, human factors. The user experience will be directly related to this realised performance as well as general usability of the service at hand. It is important to understand that the technical proficiency of the overall solution will have a bearing upon the perceived acceptability from a societal perspective. We must therefore understand the operational reality and practicality of wide scale implementations, especially where they seek to utilise existing or third party infrastructures (as with current border control aspirations for example). This is easily forgotten in discussion around theoretical benefits, as proposed by technology suppliers and consultants. We must also beware of getting lost in terms such as ‘interoperability’ or placing undue emphasis on discussion around technical standards or the theoretical performance of various matching algorithms. We should instead ensure that we have a crystal clear vision of the objectives of the broader programme, what benefits these bring for the common good, how these will be realised, why we are incorporating a biometric, what other ways of achieving the same end are open to us and how both the technical solution and the overall programme will be sustained over the longer term. These are all important questions from a societal perspective. Establishing clarity of purpose at a high level is crucially important before we delve into the intricacies of systems design.

From a societal perspective there are several questions which should be asked in relation to the provision of any such wide scale application. Firstly, setting aside whether a biometric is utilised or not, does the proposed wide scale application make sense in it’s own right? Does it provide clear benefits for the common good in the most cost effective manner? Does it take all potential users into account, including the elderly and disabled, without exclusion or ill-conceived processes? Has provision been made for adequate and suitable training for those who would administer the application through both the short and longer terms? Does the application have dependencies upon other applications or processes which need to be understood and possibly revised?

The addition of a biometric identity verification check into various aspects of the broader application should be kept in perspective. It is the host application which is important, not the biometric. A poorly conceived and orchestrated application will remain so, with or without a biometric. Adding biometric and related functionality is not a panacea for public sector applications which require identity verification. There are a host of other factors which need to be taken into consideration and properly provided for before we add a biometric. For example, the registration process prior to collecting a biometric is absolutely crucial to the overall effectiveness of any such system, particularly when orchestrated upon a wide scale. Similarly, the flow and quality of information must be properly conceived as well as closely aligned to the proposed benefits of the application. It is intelligently conceived processes, strategies and applications which will benefit the broader community, not the addition of technologies for their own sake. If these points and associated issues are not clearly understood, the image of such systems in the public perception will quickly become tainted, leading to a general dissatisfaction with their implementation. Such a situation may be quickly remedied in relation to a small, closed loop system. However, a wider scale system will require correspondingly more effort and cost in order to resolve such difficulties.

5. Human Factors and User Psychology

There are many associated issues to understand in this respect. They may be loosely grouped into the two areas of (a) operational performance and (b) the longer term societal impact. The detailed examination of these issues is outside the scope of this paper. However, we may offer a summary of how human factors and user psychology affect these two broad areas.

5.1 Operational performance

A common error repeats itself in the deliberation of many public and private sector applications which incorporate biometric functionality. When discussing and planning for performance, the discussion invariably centres around the published theoretical performance of the matching algorithms for the specific technology under consideration. Little, if any, attention is paid to environmental and human factors and how these may affect realised performance. An analogy would be to discuss the performance of an automobile engine when measured on a test bench. Naturally, it will behave differently when incorporated into a real vehicle, and differently again depending upon the payload, gearing and various operational conditions that the vehicle may find itself in, many of which are completely outside the control of the original designers. The engine is simply a component within a collection of components which provide, in this case, transportation. Similarly with a biometric check, it is simply a component among many which, together, provide a complete end to end transaction. It is the performance of this end to end transaction which is most important, both to the user and the system administrator. The term Total Systems Performance (TSP) has been coined with respect to the integration of biometrics into broader processes and should be borne in mind when considering such applications.

Human factors have a direct and significant impact upon TSP in relation to a transaction which features a biometric identity verification check. Factors such as age, gender, ethnicity, state of health and others will all have an affect. Furthermore, some of these factors are not easily classified or provided for. Consider disabilities for example. There are obvious physical disabilities which may be noted and allowed for at the time of registration, but there are also less obvious disabilities which may not be readily noticed. Degrees of autism for example, dyslexia, or those with learning or knowledge retention difficulties, as well as variations in hearing and vision capabilities. These may all make it difficult for the affected individual to reliably and consistently provide a biometric sample or otherwise navigate through an automated process. Furthermore, such disabilities may be evolutionary in their nature, making it increasingly difficult for the individual to use the system. A higher than average percentage of such users at a single point of presence will drastically affect realised performance. Add to these variations of language, a propensity or otherwise to understand technology, physiological variance and other such factors, and we can readily appreciate the significant swings in realised performance as a result. Unless these issues are properly taken into consideration, we may unwittingly discriminate against affected individuals within public sector applications, by putting in place systems and processes which they find particularly difficult to align with. Our systems must therefore be configured and calibrated with care in order to serve both the administration and the user base as well as possible, taking both security and usability into consideration. This issue is also very pertinent to scale. The larger the user base and the more points of presence involved, the greater the effect of realised performance variations[2]. To place this in perspective, the variations in performance directly attributable to human and environmental factors are typically an order of magnitude greater than the variations in performance between capture devices and matching algorithms. One might also consider this from a usage lifecycle perspective in relation to an individual. Throughout this lifecycle an individual may have a more or less distinct biometric trait, a greater or lesser interest in the overall process, a greater or lesser level of habituation and familiarity, and variance of other conditions and dependencies which may affect their ability to provide a consistent biometric sample. Such changes may also affect individual user psychology whereby an individuals' willingness to submit to such a process, even if it is compulsory, will directly affect their own performance in doing so. Transient variances in user psychology, such as mood, the effects of external pressure, diverted attention and so forth will also have a direct effect upon realised performance. In parallel, the technology itself will also evolve over this lifecycle and may affect both the user experience and realised performance.

5.2 The societal impact

We shall discuss the broader societal perspective in the next section. In this section we are particularly interested in human factors and user psychology from an individual perspective. An individual's perspective on a given application will depend upon many factors, including whether they are in general agreement with the provisions of the application, whether they have a strong political bias which affects their relationship with the agency concerned (for public sector applications), what their views may be on entitlement in relation to the process or service concerned, their own credentials in relation to the application, what personal information they are required to divulge and how they are to verify their identity. This last point is particularly important as it is at the heart of the trust model between citizen and state, consumer and service provider. With the widespread introduction of biometrics to public sector applications, we are also introducing fundamental changes to this trust model as generally perceived. Whether this is perceived on an individual basis as positive or negative will no doubt depend on how such changes are implemented and for what purpose. However, we cannot ignore the potential that such changes have to generate strong feelings one way or the other. If these feelings adopt a negative bias, then the relationship between the individual concerned and the state will be likely to deteriorate accordingly. This in turn will affect the manner in which the individual interfaces with the various processes and applications concerned. The question of proportionality arises here. If the proportion of those disenchanted by such developments is small, then this may be considered inconsequential by the administration concerned, who will in any case expect a small degree of disagreement with respect to any new process or application. If, on the other hand, a much larger proportion of citizens become concerned about such developments, then the overall success of such schemes will be seriously threatened. We must therefore pay particular attention to such matters in our deliberations and aspirations around the use of biometric and related technologies. Are we likely to immediately disenfranchise sizeable chunks of the community due to personal difficulties in interfacing with the application at hand? Will we be perceived as adopting a 'big brother' stance in relation to public affairs and treating law

[2] Further information in this context is available on the Avanti web site www.avanti.1to1.org

abiding citizens as criminals? Will individual citizens have any confidence in governmental claims made around the introduction of such techniques?

5.3 Associated human factors

We must consider some of the fundamental human factors such as ageing, ethnicity, gender and disability in relation to the operation of an automated biometric identity verification check. With ageing for example, what effect will more brittle skin have on fingerprint biometrics? Will individuals who develop arthritis have difficulty in physically using fingerprint biometric readers? Will individual's facial features change with age faster than the refresh rate of documents who carry a facial biometric? If individuals of advanced age suffer memory retention difficulties, how will this affect their ability to use biometric devices on a consistent basis?

Does ethnicity have a bearing on biometric performance? Early studies [3] suggested that further research may be needed in this respect, as it was observed that, with facial and iris recognition in particular, there were some inconsistencies in this respect. Furthermore, it is acknowledged that the incidence of specific primary fingerprint patterns varies among ethnic groups. The importance of such matters will of course increase with scale, as we implement new initiatives and enrol increasing numbers of individuals into the various schemes.

Gender may play a surprising part in some instances. There are obvious physiological issues in that many females have smaller hands and may be of smaller general stature than their male counterparts. There are also cultural issues such as the variety of female hair styles and, sometimes religious issues arise such as the tendency for females to cover their heads or faces by garments according to religious tradition. In addition, there are psychological differences which may have an impact in certain situations.

Disabilities are varied and can affect a higher proportion of civilisation than is sometimes understood. Will this affect the operation of automated biometric identity verification checks? Of course, serious physical disabilities are bound to have an impact in this respect, but there are many less obvious disabilities which may affect an individual's ability to consistently provide a biometric sample. This may be the case with mental or degenerative illnesses for example.

The tendency is to assume that individuals so afflicted represent a small proportion of citizens and that they will therefore be easily managed as exceptions. But what exactly is this proportion? And what effect will this have upon the operation of biometric devices? Perhaps more to the point, what specific provision is being made for these individuals in respect to proposed public sector applications which seek to introduce biometric technology? We must be careful not to unwittingly exclude large numbers of individuals on the basis of human factors, especially if biometric transaction errors result in denial of service.

6. The Impact on Society of the Fight Against Terrorism

In the previous section, we have touched upon the societal impact of the widespread introduction of such ideas from a personal perspective. There are many other points from which we might take a perspective. Let us consider for example a political perspective in relation to terrorism and the role of biometric and related technologies in the fight against terrorism. The terrorist threat is often quoted as one of the prime reasons for introducing widespread biometric identity verification. But do such claims really stand up to closer scrutiny and, if not, how long can such claims realistically be made in this context? No one would argue against the desirability of reducing or eliminating terrorism. However, in order to properly consider this question one must first understand terrorism, how and

[3] Ashbourn – biometric technology evaluation at University of West Hertfordshire

why it exists, how it is funded, what the associated political realities are and who is most likely to be involved. In order to address the terrorist question, one must surely understand and address the root causes. But this is not generally what happens. The majority of intelligent individuals will readily observe the duplicity of government in this respect and how political expediency often takes precedence over what many would see as natural justice. Many would be of the opinion that pardoning terrorists and convicted murderers (as has happened within Europe), or turning a blind eye to commercial interests in the supply of arms (as happens throughout the world), or befriending regimes known to be directly responsible for terrorism and the contravention of human rights for reasons of commercial expediency (including the provision of oil), hardly sits comfortably with political rhetoric around the fight against terrorism. Again, the writer is fully aware that he will not be thanked for making this point, but it is a point which must be made. The silent majority are not necessarily as unaware of such matters as some would like to think. Overstating the importance of biometrics in relation to this issue would not serve government well. Are the biometric traits of known or suspected terrorists necessarily on record? No. Would a potential terrorist volunteer this information or readily subject themselves to a related process? No. Does a terrorist necessarily need to touch a point of presence, such as an official border entry point? No. Does a terrorist necessarily have a criminal record? No. Does a potential terrorist necessarily indulge in activities to draw attention to themselves? No. Can you determine terrorist tendencies or aspirations in advance? No. Will any of the measures being introduced seriously deter terrorists or curb terrorism? No, of course not.

None of the biometrics related measures being introduced address the root cause of terrorism, and therefore none of the biometrics related measures being introduced will seriously deter terrorists or will likely alter there adherence to their chosen cause. We must be clear as to the specific purpose and anticipated benefit of any public sector scheme which introduces biometric technology and be able to articulate such purposes and benefits without resorting to broad based emotive statements about fighting terrorism. Indeed, many aspirations are already implemented and, at the time of writing, there are various terrorist related incidents occurring around the world. To overstate the effect upon terrorism that the introduction of these technologies will have would constitute a misrepresentation.

This does not mean that we should not consider how the use of biometrics and related technologies might help us in the fight against terrorism. However, we should be wary of falling back on the ‘fight against terrorism’ line when seeking to justify the widespread introduction of these technologies.

Other often quoted generalisations for the introduction of such technologies include the terms ‘security’ and ‘convenience’. Who’s security? Who’s convenience? How will the fact that a government agency holds a biometric trait of mine in a database somewhere increase my security? It will not. The problem in rising crime is centred around the failure of law enforcement to deal with it and, in broader terms, the failure of society to provide levels of education and natural justice which would negate its attraction. Once again, the introduction of technology is not addressing the root cause of the problem.

Similarly, with emotive subjects such as immigration and asylum. Providing asylum seekers with a biometrically equipped identity card may well provide benefits in guarding against multiple applications, but it will not address the primary problem of mass ‘economic’ migration. The fault lies not with asylum seekers, but with the legislation which facilitates this large scale migration and supports it with the provision of services to asylum seekers which many consider inappropriate, especially if they impact existing societies in a negative manner. Claiming that the introduction of biometrics will somehow solve the asylum seeking and immigration issue, as is often reported in the media, is singularly inappropriate.

Generalisations are not acceptable. If government perceives worthwhile applications where the introduction of such technologies can provide solid benefits for the common good, then government should specifically describe such applications, why they are being considered, precisely what the benefits are, what the costs will be and how such schemes integrate into existing processes. Honest and detailed communication, coupled where appropriate with proper consultation, would do much to inspire confidence in related aspirations. In certain parts of the world this has not happened. Instead, sweeping generalisations have been made about creating safer societies, defeating terrorism and so on. This has served to create divisions in society where certain sectors do not see an equitable equation between sacrificing what they see as elements of personal freedom and the proposed benefits to society.

We must also acknowledge the broader and longer term societal implications. If large sectors of the population come to feel disenfranchised, discriminated against, subjected to unreasonable levels of surveillance, or treated like criminals, then some will undoubtedly start to live up to the image. Measures introduced in order to curb criminal or anti-social behaviour could well have exactly the opposite effect as increasing numbers of ordinary citizens start to question their respect for authority.

Many would argue that the answer lies less in control and more in education. Clearly we need a certain degree of control, but this should not be perceived as working against the common good, or as simply an instrument of government with which to exploit citizens. The balance must be carefully judged, with the emphasis on striving to create a better quality of life for ordinary citizens and future generations. Furthermore, this balance is not just a question of technology and associated process, but should also encompass intelligent, just and responsible legislation. Indeed, one might say that it starts with intelligently conceived legislation which acknowledges the longer term position of the societies involved. Isolated projects which do not reference a broader, longer term vision will be unnecessarily constrained in their effectiveness. From a European Union perspective, placing current aspirations from individual member states into the context of a longer term (25-30 year) broader societal vision would surely be pertinent and, no doubt, illuminating. Further aligning this comprehensive vision with existing and proposed legislation (across the board – not just security or identity related, but encompassing health, education and other areas) would also seem worthwhile. Many would say that this would be a better way forward than rushing headlong into a brace of uncoordinated initiatives.

There are many potentially positive aspects associated with the intelligent use of biometric technology which, if properly and clearly explained, may be socially acceptable on a broad scale across the European Union. The issue at present is that government agencies are perceived as rushing to implement biometrics, for every application they can think of, on the back of vague generalisations around security and the war against terrorism. This is simply not good enough. Such an approach, apart from being rather disingenuous, is likely to foster confusion and mistrust. This is a great shame as there are certainly many good things we can do with the technology, which would indeed be in the broader public interest. From a societal perspective, we therefore need to concentrate on better communication and better management of associated programmes in order to demonstrate that government aspirations are considered predominantly for the common good. This improved communication should include more public consultation and a willingness for government to listen to and understand the concerns of citizens. We shall probably find that such concerns are less about biometric technology per see and more about the proliferation and use of personal data.

7. Immigration and Border Control

In the light of current initiatives, both within the European Union and beyond, it is pertinent to focus upon immigration and border control as a highly topical example of the widespread introduction of biometric technology with respect to public sector applications. This area may broadly be considered with respect to two primary activities. Firstly, provision of the new generation ICAO passport incorporating a chip and up to three biometrics. Secondly, various aspirations around the sharing of data, traveller profiling, enhanced API (advance passenger information), direct access by government agencies to airline systems and related issues.

It should be stressed that, while many associate the post 2001 interest in biometrics with security and combating terrorism, in fact, there were aspirations and trials long before this date. A significant difference is that previous ideas focused heavily on traveller facilitation while later ideas have focused heavily upon security and law enforcement. The original focus upon facilitation was certainly pertinent given the importance that travel and tourism plays in many countries from an economic perspective. If we introduce complications or societal concerns into this process, then we must accordingly consider the potential impact from a commercial perspective. It is evident that this reality has already been acknowledged in America where those involved in tourism have noticed a hesitance among non-business travellers to visit the country in light of media coverage around the US Visit and related programmes. This effect may be relatively small in scale at present and will no doubt resolve itself to it's own level in time, but it is a factor which should be taken into consideration none-the-less. Some would argue that enhanced security and traveller facilitation go hand in hand, but this is not necessarily the case, as so much depends upon the detail of implementation. Inadequately considered initiatives could easily have the dual effect of negatively impacting traveller convenience and perception while failing to offer any enhancements to security in real terms. Properly considered initiatives, on the other hand, will acknowledge that it is much more than the application of technology; and that we must strive to introduce such ideas in an ethical, responsible and sustainable manner without undue inconvenience and prejudice to legitimate travellers. This will involve close attention to operational processes and responsibilities as well as technical infrastructures. In this respect, it is unlikely that external consultants will be able to offer comprehensive solutions which are sustainable over the longer term. And yet, many government agencies are turning towards external consultants, or hiring individuals from technology suppliers, in order to shape their aspirations in this direction and rush towards implementation. It is the opinion of the writer that this strategy is seriously misguided. This is an important area we are dealing with. It is the responsibility of government to fully understand the various issues and implications and ensure that it's longer term strategy has been properly considered in this respect. This is particularly the case with regard to immigration and border control.

Let us consider for a moment the new generation ICAO travel documents. There has been a great deal of discussion around the technicalities of this document, although some would argue that unfortunate compromises have been made in the adoption of images of the chosen biometric trait rather than 'proper' algorithmically derived templates. Furthermore, there is an absence of clarity around the broader use of keys and digital certificates. However, notwithstanding the final specification and whatever biometrics are chosen from a national perspective, there are some fundamental questions we should ask ourselves around the potential use of these documents. We might usefully start with asking what exactly is it we are trying to achieve and why? We might then proceed to understand the infrastructural requirements necessary to support our aspirations.

If the main purpose of the new generation travel document is to have a stronger confidence that the individual presenting the document is the same individual to whom it was issued then, operationally, processes may be designed to undertake a simple one to one check (matching the biometric stored within the document with the live sample captured from the individual) at a point of presence, such as a self service or attended kiosk for example. Such an operation would not store or transmit the captured biometric data as there would be no need to do so. It would simply discard the data after the transaction was completed. The writer believes that the majority of citizens would find such an operation socially acceptable and feel that an identity verification check at the time of document usage is a reasonable requirement. From an infrastructural perspective, this would also be straightforward as the equipment at the point of presence would not need to locate and search a database in order to verify a biometric. Furthermore, the potential for errors with such an approach is reduced as there are less infrastructural and communications components involved in the chain. This approach is recommended therefore on the grounds of both simplicity and acceptability[4].

[4] Explicit examples of how this might work are explored in the Securing Our World document (Ashbourn)

If, on the other hand, we wish to capture a biometric and send this data to a remote location for matching against a database, watch-list, or other sundry processing, then this is a different matter entirely. Firstly, there is greater technical complexity to understand, including the variability of data already in the database and what this means to the result. The communications channels involved and the usage of third party networks where applicable. The timings of such transactions and how this relates to the user experience.

Secondly, and more importantly, we are now sending personal data across a network to what may be a known or unknown source. If the data is being processed by another administration, in another country perhaps, we have no idea as to who really has access to this data and to what purposes it will be put. What we do know is that several administrations have hinted at sharing data between governmental and commercial databases and involving third party commercial concerns in the processing of such data. This is very worrying and such an approach is contrary to the principles of data protection and privacy as articulated in many member states. The writer believes that such an approach will be socially unacceptable to many citizens. If enforced without user consultation or choice (as is currently the case with API information), the result may be a loss of confidence in, and possibly a loss of respect for, the government agencies concerned. The distinction therefore between using a biometric to verify document authenticity and using a biometric for sundry law enforcement purposes is a significant one. Let us examine this question a little further. The majority would no doubt consider it reasonable and fair that individual governments maintain a list of individuals who they believe represent a threat to their country and exercise the right to refuse them entry accordingly. Similarly, the majority would no doubt consider it reasonable and fair that, when travelling to a foreign country, the administration of the host country exercise some control over the process via a VISA issuance or similar system, stipulating admissibility, periods of admissible residency and other factors. The two concepts working together should provide a reasonable level of control over the process if intelligently conceived. The weak link here may be perceived as incorrect or fraudulent documentation. Incorrect documentation should be flushed out within the process prior to embarkation. Fraudulent documentation is another matter, as some fraudulent documents may be difficult to spot, even by an experienced immigration officer. For example, the documentation may be technically correct but issued against a false identity – a common problem, or it may have been tampered with in order to aid its presentation by the wrong individual. This is where the new generation ICAO travel document comes in as a biometric identity verification check may be quickly undertaken upon presentation of the document. However, such a check is only as good as the original registration process.

This gives us two issues to consider. Firstly, there is the strength of our own (European member state) registration process. If this is anything other than excellent, then there is a very real possibility of providing authentic new generation travel documents under false identities. Because the biometric data will match, assumptions will be made around the accuracy of the identity involved. In addition, and contrary to popular belief, it will be quite possible for multiple documents to be issued to the same individual. If the document has been issued through legitimate channels, but to the wrong person, then we have a situation whereby government is effectively aiding and abetting fraud. Even worse, such fraud is unlikely to be detected as government agencies will assume (incorrectly) that if the biometric check returns a positive result and the document looks OK, then everything is fine. The fraudster may then be free to engage in whatever criminal activity or crime against humanity they wish in the country of their choice.

The second issue is the variability of registration processes between countries. How well do we understand and trust the registration and issuance process in country A, B and C? To a degree, this is no different to the situation with conventional passports at the present time. The difference lies in our assumptions about biometrics. There will be a tendency to assume that, if the biometric matches, this must be a bona fide document presented by the correct individual and that the identity is correct. A heavily flawed assumption which, never the less, forms the backbone of many governmental aspirations. Similarly, the often expressed view that, “we don’t really care if the identity is wrong because the individual will not be able to claim more than one identity” is also heavily flawed. At the present time, it would be perfectly possible for an individual to enrol voluntarily into several government orchestrated border crossing schemes around the world, each under a different, fraudulent identity, and not be discovered due to the lack of coordination and commonality of approach. Searching databases will make no difference as we would be searching against different information, including biometric data. Such a scam could go undetected for many years, if not for ever. This whole area needs to be properly and intelligently considered in order that we understand what a biometric check really tells us (a relationship between two instances of electronic data – nothing more) and what benefits the new generation travel documents actually provide. From a societal perspective, citizens registering their biometric data for inclusion on a new generation travel document, also have a right to understand exactly what this means and how their biometric and other data will be used for immigration and border control purposes. Also with whom such data might be shared, for what purpose and at what point. This echoes the need for drastically improved communication as outlined earlier in this document.

A vitally important area to understand and clarify in relation to immigration and border control is that of responsibilities. The tendency has been to impose more and more upon the carriers in order to collect and provide personal information to government agencies. From a data protection, privacy and even moral perspective, such a practice needs to be carefully examined. Certainly, carriers have an unquestioned responsibility to check documentation and confirm its appropriateness for the proposed journey. But carriers are neither law enforcement nor immigration agents and should not be expected to assume the role of either. Immigration agencies must be responsible for the introduction and ongoing management of any new processes implemented for their purposes. If law enforcement agencies wish to play a more active role in the border crossing process, then this should be properly articulated and communicated to citizens accordingly. Furthermore, specific processes and responsibilities should be clearly delineated at the border crossing point of presence. Aspirations to enhance the current practice of using airline commercial data covertly for unrelated law enforcement purposes will be perceived by many as immoral, socially unacceptable and oppressive. This flies in the face of every principle of data protection and privacy and will not endear government agencies to law abiding citizens.

There are some intelligent ways of using biometric and related technology with respect to border control, which may be practically implemented over existing infrastructures in a cost effective manner. The document entitled ‘Securing Our World’ offered suggestions in this context in 2003. It is attached here for reference. However, it is suggested that we beware of falling into the trap of assuming technology will replace the need for human skills with regard to border control. Those government agencies who see such developments as human resource cost cutting exercises are labouring under a serious misapprehension. We might usefully replace the expression ‘automated border control’ with ‘technology assisted border control’ in our thinking around such matters. If we concentrate on designing robust processes (such as the registration and document application process for example) then the intelligent adoption of biometric technology where appropriate will be able to enhance these processes.

The last point to make with regard to international border control is the desirability for proper coordination. This is important for both equivalence of process and equivalence of performance reasons. If, in the context of a multi-segment journey, the same individual passes and fails successive biometric identity verification checks, this will generate confusion for both the authorities and the individual concerned. Similarly, if remedial actions taken as a result of failing a biometric identity verification check are vastly different from one border to the next, this will call into question both the purpose and interpretation of the use of biometrics. Furthermore, significant differences in the user experience will not foster reliable and consistent operation. This, in turn, would be perceived negatively from a societal perspective. We must understand these issues and strive for an intelligent, coordinated approach. There is still much to do in this respect as individual government agencies often seem to cling relentlessly to their localised, departmental thinking. While it is perfectly possible to have 990 or more different variations on the use of biometrics for public sector applications in Europe, it would be much more effective to have a properly coordinated approach, perhaps orchestrated from a central point. This has not happened to date with respect to border control. The result is a plethora of completely uncoordinated schemes, sometimes even within the same mother country. It is perhaps time to stop, take a step or two backwards, and re-evaluate the broader situation. This is particularly pertinent with regard to the points made about equivalence of process and equivalence of performance. With respect to the latter, imagine a scenario where there are three points of presence at a given border point, each using automated biometric identity verification. How are the three sets of equipment calibrated? To what performance level? To what degree do human and environmental factors affect realised performance differently at the three points of presence? How is this compensated for in order to provide equivalence of realised performance? Has anybody even considered these points? In all probability they have not. Therefore we shall not be experiencing an equivalent realised performance at the three points of presence. Therefore we shall experience unnecessary errors. Now extrapolate this thinking to 150 points of presence in relation to a single border (perhaps a more representative figure). What equivalence of realised performance shall we encounter? Now extrapolate this thinking further to cover every European Union border; and to cover all of the worlds borders. If we do not have even a rudimentary equivalence of realised performance across nodes, then the confidence we can place upon the biometric identity verification process is accordingly limited. This point has been raised and options for addressing it introduced. However, to date, it has not been understood by government; partly because the focus has been in the wrong areas and partly due to a lack of coordinated thinking. The same issues will arise in relation to other public sector applications. If we address them properly in relation to border control, then we shall learn much of benefit to subsequent applications of this technology. This knowledge has to be developed by governments – it cannot be bought in from third party consultants or bypassed by contracting out operational processes to third party organisations. Not that is, if we are to do things correctly and implement properly considered applications in a responsible and sustainable manner.

The implementation of biometric technology in relation to border control will undoubtedly have a significant societal impact, both immediate and for the longer term. The complexion and intensity of this impact will be directly proportional to the care and intelligence expended in the design and implementation of the related schemes. The European Union is in a rather special position due to the number of member states represented and the external perception of the Union in the eyes of the world. It accordingly has a special responsibility, both to its own citizens and, indeed, the whole world, with respect to the thinking around international border control. Let us ensure that we meet this responsibility with a sense of duty to our citizens and pride in our ability to implement intelligent, ethical, responsible and sustainable programmes for the common good. The current race to implement a disparate collection of independent border control systems with the word ‘biometric’ in them, is not the way forward.

8. Looking Ahead

There is no doubt that we shall see a steadily increasing use of biometric technology in both public and private sector applications. Within the next decade, a significant proportion of the world’s population would have given a biometric sample for one reason or another. Whether this is a good thing or not will depend upon the intelligence applied to the development of the related applications. One of the first questions we should ask ourselves in this context is – what is it that we really want to do and why? It is surprising that such a fundamental question is not always easily answered. If there is an existing process that is perceived as working badly, then we should understand why this is before adding additional layers of technology. There may be reasons which have nothing to do with the technology being used, but which need addressing in other ways. As previously mentioned, if the host process is wrong, it will be wrong with or without the addition of a biometric. We need to address the root cause of perceived issues and not assume that the application of technology will solve everything. This is particularly the case with societal issues which may have deep rooted causes. Seeking to add layers of technological control after the event is not necessarily an effective way of dealing with such issues. If we adopt such a methodology into the future, we shall develop a society whose problems fester and grow under a surface of superficial control. We shall endeavour to exert more and more control, and the societal ills will continue to grow. Governmental rhetoric around fighting terrorism and making a safer world will continue, and the societal ills will continue to grow. We shall expend fortunes on technology, and the societal ills will continue to grow. How long can such a situation be maintained? Where are the breaking points? These are questions we should be asking ourselves.

We should understand that it does not necessarily follow that advances in technology are always beneficial. If we look at the world today we can readily appreciate that some technological developments have certainly been beneficial for the broader community. Some may have brought both potential benefits and opportunities for new waves of misuse (the Internet for example), while others have huge question marks against them (the increasing complexity and cost of IT). In rushing to adopt every new wave of technology, we inevitably loose conventional skills in the process, often ending up with higher technology but poorer quality. We have been systematically fooled into thinking that technology is a substitute for responsibility. It isn't. Within the societal context, this is readily apparent in the simply appalling levels of service experienced with the major utility providers, large commercial organisations and even government departments. In many countries, reneging on responsibilities and sub-contracting to third party contact centres or service providers has resulted in a poorer quality of life for the vast majority of citizens. Furthermore, it has served to destroy the pride taken in a job well done by visible and responsible operators. Government, aided and abetted by technology and technology providers, has often been directly responsible for such developments under the guise of cost cutting initiatives. If we are to build a European Union fit for future generations, then it is time that we changed this trend.

So should it be with the current interest (some would say infatuation) with biometric technology. Certainly, it brings some genuinely useful functionality to the area of personal identity verification. But it is a tool which must be used wisely. It is not a panacea for all our identity related ills. It will not solve problems which have been brought about by political carelessness. We are at the start of a personal identity revolution; a revolution which will forever alter the fundamental trust model between citizen and state, consumer and supplier. This fundamental change will impact our society and cause people to think differently about their relationships with the world around them. It will similarly alter the physical processes associated with these relationships.

In the case of biometrics, we should strive to keep things simple and use the technology only where appropriate to support a broader process. Used intelligently as one of several factors utilised for the purpose of verifying identity, biometrics may provide valuable functionality in relation to many applications. In this manner, we shall see an increasing use of the technology. We shall also see an increasing use of the technology in relation to other technologies such as tokens and embedded functionality. Biometric sensors will become low cost commodity items in the same way that integrated circuits and computer peripherals have. Biometric matching algorithms will proliferate with many becoming available via an open source model. The value will not be in the biometric device or the matching algorithm, but in the intelligent integration into broader systems and processes. This is where a realistic understanding of the broader societal picture is so important.

In time, giving a biometric may become commonplace. But it should only be so in relation to specific purposes, preferably entered into voluntarily by the user. If related systems and processes are properly designed and implemented, then the use of a biometric should be perceived as an attractive proposition for the user. If it is perceived otherwise, then there will probably be good reasons for such a perception. Honest communication will pay dividends in this respect. While applications will exist in both the private and public sectors, government will have a key role in shaping the ongoing use of biometric technology. In this respect, governmental thinking and associated strategy should extend over a period of at least 25 – 30 years. A roadmap should foresee key milestones and developments along the way, together with logical steps needed for their support. No implementation should go ahead without a detailed forecast of sustainability.

We are currently at a fork in the road on this roadmap. Along one path lies a random collection of initiatives, entered into without clear thinking but with much political posturing and emotive rhetoric. A few years along this path is a milestone which marks the realisation that citizens were mislead as to the true nature and purpose of these initiatives, which have failed to achieve their previously stated aims. We shall still have terrorist attacks. We shall still have drugs trafficking. We shall still have illegal immigration and we shall still have a portfolio of organised and violent crime. Citizens will wonder why they gave up their freedoms of privacy and anonymity. The result will be disenchantment and resentment towards government. Further along, with societal ills continuing to escalate (because the root causes have not been addressed) government will introduce increasing levels of control and surveillance of citizens until we are living in an effective police state. Individuals will simply be material to be exploited for commercial and governmental gain with virtually no rights of redress against the misuse of this power. At this point on the roadmap we shall be moving into a new ‘grey’ age which, eventually, will have very serious consequences.

The use of biometrics is but a single strand in the broader societal landscape, but it is an important strand as it tugs at fundamental and strongly felt principles. The European Union must rise to the challenges and responsibilities that such developments bring. Other nations have already set foot upon one of the paths described above. History will show the effects of their actions. We can follow along the same path, or we can take another path. Either way, we must decide and set our course.

9. Conclusions

The past three years or so has seen a bizarre situation whereby governments who had previously been completely disinterested in adopting biometrics for logical, ethical and well considered applications, have suddenly turned about and rushed headlong into what can only be described as a frenzy of biometric related initiatives accompanied by clouds of emotionally misleading and technically incorrect rhetoric. The driving force has of course been entirely political and aimed at demonstrating some sort of response to terrorism and national security, while simultaneously introducing vastly increased powers of law enforcement activity. Politicians have sought to ride on the back of this wave while many individuals in both the private and public sectors have been grooming themselves for career enhancement via involvement. Never before have we seen so many overnight experts ready to advise government and produce ‘solutions’ to problems which neither party can clearly articulate. The situation is bizarre indeed and might make for a good theatrical script – except no one would believe it.

The implementation of biometric identity verification represents an interesting technological challenge to be sure, but we are not children playing with technological toys. We are responsible human beings, fundamentally altering the fabric and rules of our society. Such activities may be undertaken for better or for worse. At present, the direction is unclear, with some nations introducing levels of control which they themselves would have heavily criticised in others just a few years back. Principles of privacy and data protection are been discarded wholesale. If we continue blindly along this path, where will it take us in 10, 20 and 30 years from a societal perspective? It is time to take a fresh look at this whole area.

The starting point must be a re-focusing of objectives and the acknowledgement that this is not about biometrics and technology. It is about managing the interaction between citizen and state, much of which involves *some* level of personal identity declaration and verification. The precise level should depend upon the situation at hand and the nature of any associated entitlements. This is perfectly natural and is the way things have always been. Where technology can enhance or simplify such processes, then it makes sense to carefully evaluate such technology in the context of the application at hand. All of this would be perfectly understandable and acceptable from a societal perspective.

What is less acceptable is the deliberate blurring between the provision of government services and law enforcement. On the one hand, we are dealing primarily with law abiding citizens who are exercising the right to access a service, whether it be crossing a border, drawing upon agreed social services, or something else. On the other hand, we are dealing with criminals who seek to manipulate and subvert society for their own ends. Treating everyone as the latter will not help significantly to catch or deter the real criminals; it will simply cause them a little inconvenience and force them to become a little more sophisticated in their crimes against society. However, taking this course *will* have an affect upon ordinary citizens and their relationship with government. If we are not careful, we shall find ourselves headed towards a global police state, heavily manipulated by one or two strong governments. This will not make for a better world. Quite the contrary in fact.

Alternatively, we can take a clearer perspective and understand that there are some good things we can do with these technologies, if we apply them to *specific* functions and processes where it makes sense to do so, and where such applications are developed in an ethical, responsible and sustainable manner for the common good. It is time also to bring citizens squarely into the debate. Not by carefully manipulated opinion polls, but by honest and open public discussion.

In this paper, we have made some strong points and offered views contrary to what some might perceive as being politically correct, and quite deliberately so. The dialogue to date has been heavily influenced by commercial interest and political aspirations. There has been remarkably little genuine consultation with citizens on a matter which will have a significant impact upon society. Similarly, a proper understanding of this societal impact has been conspicuous mostly by its absence from any related discussion. We have also offered some positive ideas around the use of biometric technology in relation to the currently topical area of border control (via the attached document). However, it is the recommendation of the author that any such ideas remain as ideas until subjected to proper public scrutiny and debate by those most qualified to offer an opinion. This has simply not happened to date. It is time to change our approach.