The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management

Julian Ashbourn

Background paper for the Euroscience Open Forum ESOF 2006 in Munich

July 2006

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 resulting report *Biometrics at the Frontiers: Assessing the Impact on Society* (EUR: 21585)1 was undertaken by staff from the IPTS ICT in collaboration with a number of external advisors[1].

One of the external advisors to this report was Julian Ashbourn, Chairman of the International Biometric Foundation, who additionally contributed a paper entitled The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies, which has subsequently been referenced often within the broader discussion in this important area.

The present paper is not intended to duplicate the work found in the original papers referred to above, but rather to extrapolate from that point, reinforcing important messages in light of recent developments and experiences and broadening the discussion still further. It introduces the term 'identity management' into the title, in order to encompass the wider aspirations and technologies currently being considered.

Additional background material may be found on line at www.avanti.1to1.org

[1] Bernadette Dorizzi, Paul de Hert, Jonathan Cave, Julian Ashbourn

The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management

Julian Ashbourn

Contents

Introduction

This paper is particularly concerned with the societal implications of widespread personal identity management using contemporary technologies such as biometrics, smart cards, RFID and supporting general IT. However, in order to reach meaningful conclusions in this respect, we must first place things properly in context. For this reason, the paper has been divided into logical sections which provide an overview of the more general situation, together with associated challenges, leading into coverage of the societal impact, conclusions and recommendations. This approach necessarily entails raising some of the negative issues and misconceptions around current aspirations, in order to reflect a comprehensive perspective. However, the paper should be construed not as negative, but rather a realistic view of how we might understand and meet the challenges associated with the inevitable interest in identity management and related technologies.

There has always been a requirement for identity management of course. Throughout history, various techniques have been used in order to verify the identity of an individual in relation to a specific transaction, event or other purpose. Even the principle of using a biometric is not new and was certainly understood by the Sumerians and Ancient Egyptians among others. What is new, is the increasingly pervasive nature of identity management in modern society and the intensive drive to implement related aspirations.

In which way and to what extent such initiatives might benefit society remains to be seen. Claims around defeating terrorism and organised crime, while undoubtedly attractive, are perhaps overly ambitious, as are the rafts of user benefits often quoted by those with a vested interest in developing, implementing and maintaining applications. Certainly, there is no shortage of political and commercial propaganda promoting the extensive introduction of identity management into both public and private sector applications. Rather less dialogue and objective research however is expended around human factors and the possibility of introducing negative affects upon society. This is unfortunate, as we are in fact altering the very fabric of society via identity management initiatives.

The concepts of personal identity, personal freedom, privacy and protection from the mis-use of information are hugely important within a stable and happy society. Similarly, the concept of being regarded innocent until proven guilty is a closely held ideal for many. All of these concepts are perceived as being seriously threatened by current aspirations, which are effectively changing the trust model between citizen and state. Against this scenario, we have to balance the requirements for law enforcement and protection from a broad range of fraudulent activities, as well as the more general areas of national and international security.

Understanding this broader and quite complex picture is not an easy task, especially if we extend our thinking to the longer term. Consequently, many Europeans feel that there has been inadequate public discussion around such matters, prior to the pursuit of various public sector schemes and initiatives. Furthermore, concern has been expressed around the use of, and access to, personal information, especially with respect to the possibility of public and private sector co-operations. Such a situation promotes emotive questions such as : Are we moving increasingly towards a huge ‘nanny’ state where the opinion of the individual is irrelevant? Are citizens expected to have blind faith in authority? Are we being unduly influenced by countries outside of the union? Are we in danger of creating an us and them society with government and citizens either side of a broadening divide? Such questions reflect important underlying concerns, in which the concept of identity management plays a prominent part. As such, they should be fully acknowledged and addressed by government.

History shows us that the power to identify and discriminate among individuals can be seriously mis-used at a variety of levels. We are currently increasing both the availability and extent of this power by leaps and bounds. Furthermore, we are rushing to do this with a fervour rarely seen among public initiatives. Given this reality, it is surely important that we ensure a complete, open and objective discussion in this respect. A discussion which reflects all perspectives and hopefully reaches an intelligent and qualified conclusion around the future usage of identity management technologies and associated processes. This paper encourages and supports such a discussion by focusing on some of the issues that have, to date, been rarely covered in public discussion. It will culminate in conclusions and recommendations designed to help take this discussion into the future.

Technology

It is neither appropriate nor necessary to introduce and discuss the various biometric techniques, chip and RFID technology, or related mainstream information technology within this paper. The reader may find plenty of reference material in this context elsewhere.[2] What we shall attempt to do is dispel some of the popular myths around identity management technologies (biometrics in particular), helping the reader to place matters in context and understand the broader picture. In addition, we shall highlight some of the technical challenges which we feel are deserving of wider discussion.

Dispelling popular myths around technology

1. A biometric proves that you are who you say you are. **Incorrect**. A biometric does nothing of the sort, it simply provides an increased confidence as to the alignment of an individual with a previously defined identity profile. Whether that profile is accurate, or has subsequently been distorted, is another matter entirely.
2. A biometric identity verification test is infallible. **Incorrect.** Technology is always fallible and biometric technology is no exception. Furthermore, the myriad reasons for possible failure among biometric matching processes are not universally understood.
3. Biometrics enhance privacy. **Incorrect.** A biometric in isolation neither enhances nor diminishes privacy. It is a matter of how it is used within a defined technical architecture and operational process.
4. A biometric cannot be stolen. **Incorrect.** Biometric data can easily be stolen. The question is how might it be used if it is stolen?
5. You cannot derive personal information from a biometric. **Incorrect.** You may derive personal information both from the biometric itself and the data associated with it. The latter is potentially more complex an issue, as the data may have been manipulated or extended without the knowledge or consent of the individual in question.
6. Electronic chips are inherently secure. **Incorrect.** The chip is simply a storage mechanism for data. Relative security of that data depends upon a combination of technological control and operational process.
7. A stored biometric cannot be tampered with. **Incorrect.** Stored biometric data may be manipulated in a number of ways.
8. Contemporary database technology is inherently secure. **Incorrect.** The security of stored data depends on many factors, but a database in itself is not necessarily secure. Indeed, it may be rendered notably insecure by a combination of poor controls, ill-considered links with other data sources, poor policy and a general misunderstanding of IT security principles and practices.

[2] www.avanti.1to1.org , www.ibfoundation.com , www.biometrics.org , www.bsc-japan.com

Having addressed some of the more obvious misconceptions around technology, it is perhaps worth noting that technology alone can never provide an answer to societal issues and problems. Technology coupled to sound policy and absolute clarity of purpose may well provide useful benefits, but it is the policy which is important – not the technology. It is policy which creates safe and prosperous societies with good education, health care, internal infrastructures and the other hallmarks of civilisation. If these areas are found wanting, then it is policy which is at fault – not technology. There seems to be an assumption within government that technology can be applied to societal ills as a sort of 'sticking plaster' to patch up badly conceived policies. This is especially the case with regard to identity management, where all manner of unrealistic claims are being made around the widespread introduction of identity cards, new generation passports, national identity databases and other such mechanisms which incorporate or rely upon technology.

History will show the majority of these claims to be unfounded. It is not a lack of technology which causes crime rates to soar, educational standards to plummet, social services to be in disarray, communities to be in cultural conflict, mass migration to go unchecked, natural environments to be damaged and other such causes of concern to many Europeans. Consequently, the increased application of technology will not solve these issues. It is only an enhanced and sympathetic understanding coupled to intelligent policy which can reach the root causes of societal ills and change things for the better.

We desperately need to place the use of technology in a proper perspective. Technology is interesting and, if properly conceived and implemented, may support intelligent policy. But it is policy which is important and policy which should drive technology – not the other way around as currently seems to be happening with regard to identity management.

Current technological challenges

In relation to identity management there are perhaps a number of outstanding technological challenges, some of which have been explored, but are not necessarily well understood among implementing agencies. Providing a complete listing would be outside the scope of this document, however, it may be useful to focus on one or two for illustrative purposes.

Equivalence of performance across operational nodes

In order for the citizen to experience a fair and equivalent process at disparate points of presence in relation to a given, or related service, such as border crossing, the provision of social services, public sector financial transactions and so on, it is important to have an equivalence of both process and performance.

Realised performance at a given point of presence depends upon a variety of factors including:

- The biometric match threshold setting
- The configuration of the supporting technical infrastructure
- The reliability of accessing the reference biometric
- The operational reliability and accuracy of the biometric capture device
- Human factors (including age, ethnicity, disability, etc.)
- User psychology
- Environmental factors

Without an equivalence of performance across multiple points of presence, or nodes, the user is at a disadvantage and may find themselves failing a biometric identity verification check through no fault of their own. Conversely, a poorly configured node may introduce vulnerabilities into the overall system, raising the risk of identity spoofing. Lastly, if the

operating agency cannot demonstrate an equivalence of performance across nodes, then it cannot claim an open and fair operation and is consequently exposed to counter claims.

This important issue has been raised by impartial qualified entities [3] and a possible solution has been developed and made freely available to government agencies in the common interest. To date, government agencies have not acknowledged this issue or demonstrated an interest in addressing it. As related initiatives scale upwards, the issue will however become self evident, both to implementing agencies and indeed, citizens, as regular users observe differences in the relative systems performance at different points of presence. Such an observation will do little to reassure citizens that a given application is being operated fairly and objectively.

Relative operability among biometric devices and algorithms

At present, the specifications of biometric capture devices, matching algorithms and related components are generally stated (if at all) according to proprietary methods. This makes it difficult to compare any two devices or subsystems in a meaningful manner. Equally, it makes it difficult to predict the likely performance of an application featuring capture devices from more than one supplier.

In order to address this issue a Biometric Operability Index was devised by the IBF, which would provide a common methodology with which to describe the operational performance of biometric devices and components. While a small number of technology suppliers contributed to this initiative, the majority are clearly content to continue with the current obscure methods of describing performance as their primary clients, at present government, do not seem to be requesting anything better. The result will be difficulty with the configuration of wide scale applications where multiple devices have been supplied by disparate vendors. This reality renders technical performance equivalence an even greater issue.

Other technical challenges

There are many other challenges and issues to be addressed in this context, both in relation to capture devices and back end supporting IT. Suffice it to say that identity management technology is still evolving and will doubtless change over time. In this respect a longer term technical strategy, with clear objectives and milestones, would be a useful common instrument. The nucleus of such a strategy is included within the more general longer term ‘roadmap’ devised and promoted by the IBF. It may be that the European Union could develop this idea further into a useful, agreed longer term technical strategy for identity management.

Policy and assumptions

This is a complex area and, within the scope of this paper, we shall not be able to address it in a comprehensive manner. However, we might usefully cover some fundamental points which may be considered important from a background perspective, prior to discussing the societal implications of current thinking in this area.

As stated earlier in this document, it is intelligent policy which may best address the perceived ills of society and provide acceptable and sustainable futures for European citizens and their descendants. Such policies should be developed irrespective of the status of available technology. Furthermore, clear responsibility for such policies should be in place and

[3] International Biometric Foundation (www.ibfoundation.com)

understood, including the provision of supporting research, public debate and absolute clarity of purpose. Such mechanisms are the characteristics of a democratic and fair society.

Unfortunately, we seem to have blurred this ideal via extensive consultation with commercial organisations, coupled to an un-natural focus and emphasis upon technology. This often results in the outsourcing of public sector initiatives to private sector technology suppliers, including the overall design, operational process and day to day operation. Equally, this often results in the delivery of such initiatives being seriously delayed, significantly over budget and failing to meet the fundamental requirements of the original objective. Some would say that this is a sympathetic way of referring to the unmitigated disasters which litter the track record of public sector IT related initiatives. It would be unfair to generalise as to the reasons for this situation, but one factor which cannot be ignored is the over-statement of benefits by technology suppliers. This is not necessarily the product of malicious intent, but may stem partly from a misunderstanding of the distinction between technical theory and operational reality, coupled to insufficient research and communication prior to implementation.

Within the sphere of identity management, this is a particular concern, as promotional propaganda around identity management technologies has lead to certain assumptions being made, many of which will ultimately prove to be incorrect. The issue here is what personal freedoms will have been compromised in the meantime and to what extent will this be irreversible, given the nature of data proliferation? Is there a danger that we might create an identity management nightmare, due to related initiatives being driven more by technical expediency than intelligent policy? There is already evidence to suggest that this is a very real danger.

At this point, it is pertinent to bring up the matter of strategy. What exactly is the longer term strategy for identity management within the European Union? Who is the custodian of this strategy and where might it be publicly examined? How are individual initiatives aligned and reconciled within this strategy? Where is the required and documented process which ensures that each initiative is properly considered, with an absolute clarity of purpose statement, coupled to defined benefits, costs and longer term plan? Within this strategy, where might a citizen find details of data protection policies, legal clarification and remedial processes? How does this strategy itself align to the broader international situation?

Herein lies one of the major concerns among European citizens. Without such a strategy, where is all this leading? Who is safeguarding the interests of ordinary citizens both now and into the future? How might they be reassured that a proper balance is being struck between the aspirations of law enforcement and the ideals of a democratic society? There are some serious issues here which require clarification. If European government (and that of every member state) cannot demonstrate a clear longer term strategy which ensures that identity management technologies are implemented in an ethical, responsible and sustainable manner, then it will be perceived as failing in its responsibility to citizens.

It would be an easy enough matter to construct a small governmental working group in order to develop and communicate such a strategy. However, it would be important to resist the temptation to involve technology suppliers and consultants. Already, there are too many self-styled groups, lead by technology suppliers, purporting to offer solutions to societal problems which are largely defined by themselves. When a robust strategy has been developed, then certainly we may evaluate contemporary technology in relation to it – but the strategy must not be driven by technology or technology suppliers. Government must take full responsibility in this context, and be seen to do so, if we are to achieve anything worthwhile.

Operational processes

We have already referred to the importance of equivalence of performance in relation to operational points of presence. Similarly important is equivalence of operational process across nodes. Even if we attained an equivalence of technical performance, if the overall process and in-place policy differs between nodes, then the user experience will be correspondingly different. In addition, communication and understanding of the correct procedures will be especially challenging.

Imagine, for example, that a citizen is undertaking a journey throughout Europe and, at each border crossing point, he or she is required to undertake a biometric identity verification check. Is the understanding of what constitutes a reliable match the same at each node? If the identity verification fails, what are the consequences? May the citizen make multiple attempts at verification? If so, how many? At what point is it decided that the verification has absolutely failed? What is the nature of secondary processing following a failed transaction? What other agencies are notified of such a failure? What are the rights of the citizen in this respect?
It is important that we consider such questions and develop clear operational processes which are agreed and understood by all concerned, including citizens. The same principles would apply to any application which features identity management.

Similarly, as the number of next generation passports and identity cards proliferate, the question of who can access the data held on these tokens, for what explicit purpose, and how that information may be used becomes vitally important. This will especially be the case where multiple agencies may use the same token for slightly different purposes. Furthermore, the usage of such tokens in association with back end databases raises a host of questions around data access and privacy. The identification and definition of required processes should be an integral part of a longer term strategy.

Data access specifics

If, within a single agency, multiple individuals are authorised to access personal information about a citizen, whether in association with the use of a token or otherwise, then there should be explicit operational processes in place to ensure that this only takes place under certain well defined circumstances and for specific reasons. Furthermore, access control mechanisms should be maintained and regularly audited in order to ensure compliance. If this is not in place, then we have effectively lost control of the data and privacy is compromised.

If multiple agencies within the same country are authorised to access this information, then creating, maintaining and enforcing such processes becomes considerably more difficult. The likelihood being that we shall very quickly lose control of the data. We have seen many instances of this scenario already.

If multiple agencies within different countries are authorised to access this information, then there is no effective control over the data and privacy will certainly be compromised, especially where the countries involved maintain a slightly different cultural and political profile.

If the above conditions are extrapolated to include access to personal information within government databases by commercial organisations, then there is no control whatsoever over the data.

To even suggest that the privacy of personal information will be respected under such conditions is slightly ridiculous. Already we have a huge problem in this respect, and the addition of ever larger identity management databases will exacerbate the existing situation. It

is not helpful to deny, or shrink from this reality. We must strive to improve operational processes and establish strong mechanisms to protect the personal information of our citizens. This should be the first priority within any related initiative.

Security and the global perspective

There are many shades of security, from personal to international, from physical to informational. It is difficult, if not impossible, to address them all in a general sense, and yet this is often exactly what happens in media coverage and political rhetoric. Phrases like 'such measures will enhance security' and 'for your protection' are far too wide to be meaningful. We desperately need clarity of definition and clarity of purpose, especially with regard to identity management proposals.

Let us start by considering the emotive subject of terrorism. The term has particularly come to prominence in late 20th and early 21st century life as a recognised factor within global civilisation (although one might argue that the concept of terrorism goes back much further). Terrorism may be politically inspired, or may be a product of religious fundamentalism, or may even be commercially driven. A common thread seems to be that those perpetrating such crimes have little or no regard for the views or welfare of others and are prepared to take extreme measures in order to pursue their own objectives. The reasons why individuals decide to go down this path are no doubt complex. Babies are not born terrorists. Something happens in their experience which causes them to adopt such a lifestyle. Perhaps it is the influence of others. Perhaps it is frustration with their surroundings, their individual progress through life, or maybe even their personal relationships. However, it is unlikely to be because they don't posses an identity card.

Organised crime similarly takes many forms, but is mostly driven by commercial gain and power. It is often, but not always, accompanied by violence. Indeed, many would argue that there is a fine line between organised crime as is popularly understood, and the business activities of many of the worlds largest corporations. Similarly, bribery and corruption in public office has many parallels. What attracts individuals to this particular way of life? Again, babies are not born criminals or corrupt businessmen and politicians. Something happens to them along the way. Perhaps it is the prospect of easy money, or the vanity of position and power. However, it is unlikely to be because they don't posses an identity card.

Then there is the lower level opportunist or habitual crime, which may be driven by a number of causes, such as poverty, lack of education, or perhaps an inability to achieve fulfilment within a complex world. No doubt criminal psychologists could come up with a thousand reasons why an individual follows this path. However, it is unlikely to be because they don't posses an identity card.

The primary point here, is that individuals do not ordinarily become criminals or terrorists due to a lack of technology, and especially not due to the lack of an identity card or entry within an identity database. Consequently, the provision of such technology is unlikely to change either their views or lifestyle in any positive manner. Indeed, ironically, it might cause them to become more focused, proficient and expert in their chosen endeavours.

Each of these individuals was somebody's precious child, carried by their mother and laboriously delivered into our complex world. They have subsequently been influenced or persuaded to follow a direction contrary to the common interest. Understanding precisely how and why this happens is our key to reducing the affects of organised crime and terrorism, by addressing the root cause with intelligent policy. Simply increasing the extent and powers of

law enforcement upon ordinary citizens, with technology and associated legislation, cannot produce a satisfactory longer term solution to these problems. They are simply too complex and deep rooted to be addressed in this way.

However, we do of course need law enforcement and judiciary procedures, in order to protect our citizens against both opportunist and organised crime. Herein lies the challenge. The majority of law abiding Europeans would no doubt consider it reasonable to use all the technological tools at our disposal in order to prevent crime or apprehend criminals. However, they don't want to reduce Europe to a police state in the process. Many are of the opinion that the 'surveillance society' has already gone much too far. The attention of police forces and law enforcement agencies seems, to many, to be unnaturally focused upon ordinary citizens and not upon criminals. This perception is reinforced by the visible failure of the same agencies, often to resolve incidents of serious crime. Furthermore, the judiciary is often perceived as being more on the side of the criminal than the victims of crime. Within such a framework, the imposition of extensive identity management within society is unlikely to be viewed in a positive light. There may indeed be positive uses for such technologies, but without intelligent supporting policy, the impact of implementation could become negative.

When we consider the truly global situation, including international terrorism and national conflict, security, and indeed identity management, adopts a slightly different complexion. Naturally, administrations will be keen to identify known terrorists and their movements. However, known terrorists are unlikely to volunteer for membership within law enforcement databases. If they are already resident, the identity profile may or may not be correct. There are many perspectives to this. One might argue that, if such individuals are known, then why are they not apprehended? Is international law enforcement simply not up to the task? Could it be that the unknown individuals, or 'sleepers' pose an equal or even greater threat? If so, it is likely that they will have perfectly legitimate credentials. How will identity management meet this threat?

In areas of national conflict, which may or may not lead to outright war, how exactly would the power of identity management techniques be used? No doubt it would depend on who is wielding it and why. National conflicts in living history around the world, show us that such a power is unlikely to be used in a sympathetic manner. Indeed, it seems that many crimes against humanity involve the identification and discrimination of individuals, often those ill equipped to defend themselves.

The root causes of national conflict run deep and may be inspired by a number of factors including the control of resources, cultural differences, political agendas, poverty, and a more general desire for change. Undoubtedly, the key to reducing the likelihood of national conflict, is to understand and address these root causes. It is unlikely that one of them will be a lack of identity management. Consequently, it is likely that the application of intelligent policy will have a more beneficial effect than the application of identity management technology.

The above paragraphs stress the need to place technology in general, and identity management technology in particular, in a proper perspective. Such technologies should not be promoted as the answer to all of our security related problems. They are not. The social ills and pressures we are experiencing within the European Union and the rest of the world are a product of poorly conceived policies and poor management. If national crime rates, terrorism and social dissatisfaction are soaring, then it is because we are not managing these factors well enough. The political assumption, that we can somehow apply a 'sticking plaster' of technology to these social ills and that they will consequently be alleviated, is seriously flawed. That is not to say that there isn't a place for such technologies, but we need to be much more specific as to their true purpose and value. In this respect, we are currently found wanting.

Human Factors

The broader issues around human factors have been covered elsewhere[4] and there is no need to delve too deeply into this area within this paper. However, it is perhaps worth re-visiting the fundamentals as general background to the main theme.

Human beings come in all shapes and sizes. The closer one looks, the more individual they seem to be. This, indeed, is the foundation for utilising techniques such as biometrics. Moreover, this individuality is more than skin deep and user psychology can play a large part in the realised performance of a biometric identity verification transaction. Similarly, nature has endowed us with a direct link between the psychological and physiological, with thoughts and emotions producing distinct physiological responses. This, in turn, can have a significant effect upon the realised performance of an identity verification transaction. This is not a matter of hypothesis, but has been proven time and again in systematic observation.

In addition to the above, we have the issue of involuntary variation, such as age, ethnicity, illness and disability. The sum of all these variables results in a complex interaction between human beings and identity management technologies. While the human interaction with technology is always interesting, it is particularly so with regard to identity management, due to the complex factors outlined above.

As a result of human factor variabilities we shall find some individuals for whom, through no fault of their own, biometric identity verification simply does not work well, or perhaps, depending upon the technique chosen, not at all. Consequently, we shall always need to provide fallback procedures and manual processes for those who cannot reliably interact with identity management technologies. This situation is at least unambiguous. More complex is the situation whereby individuals who, ordinarily, can interact successfully with such systems, prove to be inconsistent in day to day transactions. This can be for a variety of reasons, including variations in the quality of reference templates, user psychology, user physiology or a lack of technical equivalence between operational nodes.

Understanding exactly why a biometric identity verification transaction has failed is not easy. Especially where the failure might be borderline, but the system in use does not provide an indication of this. This is an interesting point. The majority of operational systems deployed to date, do not have sufficient granularity in their interface to indicate how close a matching transaction is to the match / no match threshold. Instead, they tend to simply employ a binary pass or failed methodology. Similarly, the assumption among many operators is equally binary. They assume that, if a biometric identity verification transaction is successful, then it must be the right person or, conversely, if it is unsuccessful, then it must be an impostor. Such thinking, both from an operational and systems perspective, does not adequately take human factors into account. There may be perfectly good reasons why an individual consistently fails an identity verification test at a specific point of presence, on a specific day, or according to specific local circumstances. Such a failure does not necessarily mean that they are an impostor, just as success does not necessarily mean they are who you think they are.

It may take time for those in public service to come to really understand the human factor variables and how they affect identity verification performance. After all, they have not previously had to work with these technologies. In the mean time, there is much that could be done to clarify this complex area.

[4] See www.avanti.1to1.org for example

Societal impact

So far, in this paper, we have given a brief outline of some of the important factors to be taken into consideration within the broader identity management discussion. This is necessary in order to set the scene for our deliberations around the societal impact of the widespread introduction, indeed, globalisation, of the identity management concept. We must consider the broader picture, both now and into the future, if we are to ensure that identity management is utilised, where necessary, in an ethical, responsible and sustainable manner which serves to safeguard the interests of citizens, rather than become an imposition upon them. In this respect, while there may well be some very positive applications for identity management, there are also some very real concerns and potential dangers. We are dealing here with the very fabric of society, and must ensure that we do not erode the quality of life for our children and grandchildren, under the guise of reacting to security issues.

Law enforcement

It should be acknowledged that one of the primary drivers for the proliferation of identity management is law enforcement. Law enforcement agencies, perhaps understandably, feel that their task would be easier if the entire population were tagged, present in a biometric database, and tracked wherever they go. This way, they could more easily match forensic evidence with possible suspects and have a better chance of apprehending those suspects. Furthermore, they believe in the globalisation of identity management and the sharing of national databases in order to further facilitate this law enforcement ideal.

From the citizens perspective, there are aspects of this model with which they are, generally, uncomfortable. Firstly, it assumes that everyone is a suspect and therefore guilty unless proved innocent. This is directly contrary to what they see as one of the important tenets of a free democratic society. Secondly, it requires that decent, law abiding citizens be treated as criminals, with their fingerprints (and/or other biometrics) taken against their will and held in criminal databases. Furthermore, such data will be readily shared among law enforcement agencies both nationally and internationally, without the consent or even knowledge of the individuals concerned. Thirdly, it is possible that serious identity related mistakes could be made and, given the unreasonable assumptions being made as to the value of a biometric, innocent individuals could find themselves accused of crimes with which they had absolutely no connection. Moreover, disproving the incorrect assumptions around a biometric match might prove extremely difficult. Fourthly, there is concern among many European citizens that we are creating a virtual police state, wherein law enforcement agencies are coming to see citizens as the ‘enemy’ rather than seeking to serve their interests. Those who would consider such concerns as overly emotive, or even scare-mongering, should appreciate that much of this scenario is already in place and being actively pursued.

From the above, we may appreciate that there is a very real potential for law enforcement agencies to alienate themselves from decent citizens, eroding the goodwill and community support which they have traditionally enjoyed. This is a very serious matter indeed. It could lead to a society where there is no natural respect, either for authority or for the individual. We are already seeing advance signs of this, with spiralling crime rates, even though law enforcement, in many European member states, has effectively been strengthened. A good example is the United Kingdom where, in spite of becoming a ‘surveillance society’ serious crime is rife and prisons overflowing. It is often reported that many decent UK citizens have lost confidence in a law enforcement system which they see as largely ineffective, and a judiciary system which seems to favour criminals over the victims of crime. Imposing an unwanted identity management regime upon these same citizens will do little to restore their faith in either law enforcement or government. Citizens of other member states may have

slightly differing perspectives depending upon their personal experience and understanding of law enforcement in the national, European and International arenas.

This is undoubtedly a thorny area. It is natural that law enforcement agencies should use contemporary technology where it helps them to fight crime. However, there is a need for intelligent control and clarity of purpose. We must balance the effective use of technology against the impact of over zealous or unsympathetic deployment from a societal perspective. Many Europeans will be of the opinion that identity management techniques should certainly be used in association with serious crime, but that there should be a distinction between identity management in respect to known criminals and decent, law abiding citizens. If this balance is correct, then there will no doubt be benefits which may be realised. If the balance is incorrect, the disadvantages may come to heavily outweigh the advantages.

There is another, perhaps even more worrying, factor with regard to what might be perceived as the creation of a virtual police state. I refer to the impact upon the younger generation. In particular, those individuals who are at a point in their lives where they may be easily influenced and orientated towards one path or another. If they feel that they are growing up within an over-bearing, uncaring society where they are already treated as criminals, then they may respond by living up to expectations and behaving like criminals. Such behaviour can be infectious among those who may feel frustrated with their position. In addition, it seems that this situation is no longer associated exclusively with the under-privileged or those from troubled backgrounds, but can occur in a more widespread fashion, as is already evidenced. If we mix in the reality of many millions of economic migrants with different cultural perspectives who may similarly feel at odds with mainstream society, then the potential for creating an us and them situation is very real.

There are no easy answers to such complex issues. The root cause of many of the pressures which turn people the wrong way comes back to poor governmental policy. Over-population, inadequate education, corruption in office, poorly aligned social services, ill-balanced judiciary procedures and other factors all create tensions in society. Such tensions can lead to disillusionment and point impressionable individuals in the wrong direction. We can only counter this with more intelligent policy and the creation of a fair and just society. Law enforcement agencies therefore have a difficult path to tread. They must, of course, endeavour to maintain a secure environment, using the available tools at their disposal. However, meeting this responsibility will be much more difficult if they lose the support and goodwill of ordinary citizens. They must not assume that technology is the answer to all their problems – it isn't.

The effectiveness of ongoing law enforcement within the European Union will be largely proportional to the degree that intelligent processes are in place and traditional law enforcement skills are being practiced. The current interest in identity management should therefore be placed firmly in context and full consideration given to the broader picture and, in particular, the position of decent, law abiding citizens. If we are unsympathetic to this situation, we might, even with all the latest technology, be effectively taking several steps backwards. Alternatively, with an intelligent application of contemporary technologies, law enforcement agencies may be able to enhance both their effectiveness and their perceived profile among citizens. The key lies in clarity of purpose and the intelligent matching of technology to specific tasks, without allowing function creep of any kind. Such an approach is entirely feasible and, if pursued in a systematic and properly planned manner, could result in significant benefits to both law enforcement and the broader community. This must surely be the way forwards.

Governmental control

What is the purpose of government? Many Europeans would no doubt suggest that, within a democratic society, the purpose of elected government is to represent the views of citizens and to manage national and international affairs on their behalf. It is unlikely that many would suggest that the purpose of government is to impose its own, separately developed, view upon citizens and to exploit them according to its own agenda. And yet, this is often how government is perceived with regard to its handling of identity management.

There seems to be an assumption among government that increasing control over citizens is a good thing and that, as identity management techniques significantly enhance such a control, then they must also be a good thing. The situation is exacerbated by technology suppliers who lobby government with all manner of 'visions' which promise the identification and tracking of citizens at all times, linked to their private activities and transactions, in order that government agencies may know everything about every individual and their movements from cradle to birth. Politicians eagerly receive such ideas and are seemingly prepared to spend billions of euro (of taxpayer's money) in order to rush to implement any such scheme without properly considering the consequences and without a proper public debate. Does anyone stop to stand back and ask the question, why? How is this going to make the world a better place? It is simply not good enough to fall back on generic phrases like 'enhancing security' or 'protecting our borders' or 'controlling immigration' all of which are issues resulting from poor government policy in the first place. The broad assumption that exerting such a level of control over decent, law abiding citizens is going to solve such issues is clearly nonsense.

In 10 and 20 years time, regardless of the proliferation of identity management within the European Union and beyond, we shall still have terrorism. We shall still have violent and organised crime. We shall still have crime against women and children. We shall still have drug trafficking and people trafficking. We shall still have corruption in public office. We shall still have illegal immigration. The proliferation and globalisation of identity management is not going to solve these issues, because it is not a lack of identity management that causes them in the first place. Such issues may only be diminished and resolved by the application of intelligent government policy. Currently, such policy is conspicuous by its absence. As is variously reported in the media, we have in Europe today governments who have granted wholesale amnesty to terrorist organisations, governments who willingly allow the supply of arms and munitions to administrations who commit crimes against humanity, governments who have given convicted murderers senior posts in public office, governments who routinely allow serial killers, rapists and child molesters to walk free and re-offend, governments who donate huge sums of taxpayers money to external causes while their own health and education systems lie in ruins. Do we really think that, by some miracle, these same governments are going to solve the societal issues referred to above, simply by the imposition of identity management regimes upon law abiding citizens?

As has been stated several times in this document, it is only intelligent and well conceived policies which can have a positive impact against such societal ills. So long as such policies are absent, so long shall we suffer from the effects of these conditions.

In light of the above, one might well look towards the future and consider what the longer term holds for European citizens and their descendants. European ministers and politicians may like to do the same. It is perhaps time for a change in the way government sees itself in relation to the broader community. If we are to have any notable success in tackling societal ills, we will best do so as a unified community, not as a community divided between government and citizens. At present, the trust model between government and citizens is in danger of being seriously eroded. If not properly managed, identity management could become an instrument of destruction as far as this model is concerned. It is the wise government who will understand this point.

Commercial exploitation

Any situation which involves a step change in society or the use of technology is bound to be exploited from a commercial perspective, regardless of the longer term implications. The proliferation and globalisation of identity management is no exception, and technology suppliers are lining up to take advantage of the situation accordingly.

This exploitation will manifest itself broadly in two ways. Firstly, there is the supply of technology and systems to government agencies, itself a major opportunity for technology suppliers, systems integrators and consultants. Naturally, they will all say whatever they believe government wants to hear and, of course, they will all have the optimal solution for any problem you care to mention, whether real or imaginary. Secondly, there is the service industry who, if given access to personal information in government databases, will seek to exploit this information from a marketing perspective, no doubt re-compiling and re-selling lists of personal information, even to a greater degree than they do today. The result will naturally be a complete lack of control over personal information, who has access to it, and for what purpose.

Another development will be the insistence of biometric identity verification checks for commercial transactions and processes, whether warranted or otherwise. This could easily spread to the point where a citizen is required to give their biometric and have their personal data accessed for almost every interaction with a third party. At first, the ill-informed may believe that this somehow makes them more secure. However, it will eventually occur that it is really all about marketing and exploitation of information and, in fact, there is a very real possibility that, with the proliferation of readily accessible personal data, the individual may actually find themselves vulnerable to new risks and security threats.

Commercial exploitation can be distasteful when monetary gain takes precedence over ethics and it is wielded to the detriment of society. We see this manifested in many ways, from business cartels to environmental damage, and even in the manipulation of ideals. It is particularly worrying when it touches individuals on the wide scale that is anticipated with the effective globalisation of identity management. In this respect, it will be important to ensure that proper controls are established to check the mis-use of data for commercial reasons. Ultimately, this will become a serious issue and we should be very careful as to the accessibility of personal information in relation to everyday transactions.

Erosion of privacy

The erosion of privacy, increasingly experienced by citizens in Europe and beyond, has become a worrying issue for many. It is hardly surprising that organisations have surfaced around the world to highlight this situation. Governments speak of the right to privacy and the various in place data protection acts, as though they were keen to protect citizens in this context. The irony is that it is predominantly government who run roughshod across every principle of privacy and data protection. Witness the provision of API information for travellers between certain borders and how this has increased in both content and geographical coverage in recent years. Witness how some governments, the United Kingdom being an example, have readily sold citizens personal information to the commercial sector, without either the consent or knowledge of the individuals concerned. How can the same governments maintain any serious pretence at safeguarding citizen’s data? This is particularly pertinent with regard to the establishment of national and international identity databases.

The truth is, there is no such thing as privacy and the protection of personal information any more. The attraction of data exploitation for commercial gain has evidently been too strong for both public and private sector organisations to resist. The result is that your personal information has been set loose and now resides within a multitude of databases, the majority of which you are not even aware of. Exactly how that information is being used, and by whom, is something you will also never know. This is the problem with the proliferation of data. Once it is out of the box, you have effectively lost all control over it, regardless of how many data protection acts politicians may like to wave in the air. This is the reality. However, this does not mean that we should not strive energetically to highlight the ongoing erosion of privacy and the mis-use of personal information, insisting that proper controls are established in relation to any and every new initiative in this area.

The irony is, that as the volume and accessibility of personal information increases, the quality of that information is likely to decrease proportionately. This is a universal law. Each time such data are used, there is a possibility that they will be manipulated in some way or another. This may take the form of copying the data to other sources, updating individual records, appending information, wrongly linking informational items and so on. Furthermore, with the advent of automated profiling techniques, the data could be quite incorrectly associated with perceived risks, whether from a commercial or security perspective. The result is that we shall be drowning in a sea of data. Those with questionable aspirations will be quick to spot this reality and exploit it with a vengeance.

The citizens perspective

It is interesting that, in an area as fundamental to society as identity and identity management, the views of the citizen seem to be largely ignored. Carefully manipulated 'publicity' exercises where a limited number of citizens are asked leading questions, mostly with deliberately emotive content around security, are both misleading and potentially dangerous, in that they obscure the really important issues. The truth is that many European citizens are genuinely concerned about developments in this area, and that this concern, to date has not been properly addressed by government. However, it is not too late to do so.

Much of this concern is not so much about identity tokens, but the lack of information being given about the back end databases and how such information will be used. When decent, law abiding citizens express concerns around being treated like criminals, such concerns are often ridiculed by government or met with disingenuous comments such as 'if you have nothing to hide you have nothing to fear'. This is not good enough. Actually, decent, law abiding citizens have good reason to be concerned, with their personal and biometric data entered into, or otherwise referenced against criminal databases. Furthermore, this is happening across borders, for example between Europe and the United States, making it effectively impossible for citizens to determine how their personal data is being accessed, by whom, and for what purpose. This is against every principle of privacy and data protection.

The other primary concern among citizens lies in the relationship between citizen and state. While understanding the requirements for security, many citizens nevertheless feel concerned, and even threatened, by what they perceive as an increasing interference in their life by the state. This is particularly pertinent to identity management. Citizens are wondering exactly why government is so intent on introducing identity management schemes. Few are naïve enough to believe that such measures are going to have a significant impact upon terrorism, organised crime or illegal immigration, the often given reasons for their introduction, so what are the real reasons behind these developments? Furthermore, they are concerned around scope creep and the negative possibilities that are enabled via the establishment of identity management infrastructures.

Such concerns are not the ramblings of extremists or those with hidden political agendas. They are genuine concerns from responsible citizens who have become somewhat disillusioned, both with the governmental usage of information in general and the ability of government to remain loyal to original concepts and associated reassurances. Such concerns will not go away unless they are properly acknowledged and addressed.

On the other side of the coin, many citizens will readily see that the introduction of identity management techniques, in a controlled manner and for very specific purposes, could have a positive value for society in general. The issue, as has been previously stated, is one of clarity of purpose. A specific scheme, introduced in order to resolve a specific issue, may have such benefits, provided it is properly balanced against risk, restricted in scope and maintained with clear controls and accountability. The problems arise in parallel with aspirations to link databases, share data and blur the line between public and private sectors.

There are intelligent ways of designing and implementing responsible schemes which would make them quite acceptable to the majority of citizens. It is not the technologies which people fear, but the irresponsible and unethical usage of them. The way forward is for both government and the private sector to start demonstrating that they can design and implement identity management systems in an ethical, responsible and sustainable manner, not just for today, but for future generations.

After many hundreds of years of distinguished development in Europe, citizens have come to expect a certain quality of life. Indeed, many millions of them fought and died in terrifying wars in order to preserve and protect such ideals. They have a right to expect a certain continuity of civilisation and that their elected governments will endeavour to provide the same. Nowadays, many of them see the very fabric of such civilisation being eroded, with soaring crime rates, the systematic destruction of local culture, the abandonment of long held values and a raft of other societal ills. Moreover, they do not see how the imposition of wide scale identity management will reconcile these ills. Indeed, they are concerned that such measures are simply moving us all towards a virtual police state. This is not what their ancestors fought and died for. Governments would do well not to underestimate the depth of feeling in this respect.

From the citizens perspective then, much needs to be undertaken to reassure citizens as to the true nature of existing and proposed systems, exactly why they are being implemented, what is happening with their personal data in the background, and what the longer term strategy is.

The sinister side

Identity management is largely about control. Control of who goes where and what services and entitlements they may access. In public sector applications, such as border control and access to social services, the control is exercised by government over citizens. Substantially increasing the coverage of public sector identity management, substantially increases this level of control. Furthermore, this scenario enables a significantly increased ability to track individuals by both transaction and movement, establishing a detailed audit trail accordingly.

Many would argue that such a level of control is unnecessary within a civilised democratic society. Moreover, if such a level of control is established today, how might it be used tomorrow? Especially if the countries and administrations involved find themselves in conflict at some point in the future – not an unrealistic scenario.

The levels of control currently being established will quickly destroy any notion of privacy. Citizens will be traceable at every point and readily segmented by whatever criteria the controlling agency chooses to adopt. Such criteria may be related to age, gender, ethnicity,

religion or social history. This amounts to a power to discriminate at will and at speed with regard to huge populations. How such a discrimination may manifest itself in practice one can only speculate upon. However, history shows us that the likelihood is that such discrimination will be used as a weapon.

We also have the area of social engineering to consider, whether from a political, religious or even commercial perspective. The use of personal information in this way is entirely predictable once it has proliferated to a point which makes such exercises seem attractive.

We must also consider the 'snowball' effect where the sheer amount of available data increases exponentially as related schemes are established. This information will not evaporate of its own accord, but will sit there in cyberspace indefinitely, unless conscious efforts are made to remove it. The likelihood of this happening is remote, as no-one will ever understand to what extent information has been copied, transferred to other lists, recompiled, amended, or manipulated in other ways. The Internet already shows us a good example of this phenomenon, where information posted at the early stages of implementation may be found in various disparate sources, completely outside the control of the originator.

The current feeding frenzy, for that is how it is best described, around identity management by both government and technology suppliers has, to date, failed completely to take an intelligent view of the longer term implications of current aspirations. This bizarre rush to implementation will result in situations developing which are largely irreversible and potentially damaging to society in general. This is not a good thing.

The positive side

Given the inevitability of technology being utilised once it has surfaced, we have a social responsibility to ensure that, in the case of technologies which may negatively impact society, we at least strive to implement them in an ethical and responsible manner. With regard to identity management, there are undoubtedly some very positive applications which would be accepted as being in the common interest, provided they are properly designed, initiated and maintained. The key lies in clarity of purpose and responsibility.

For example, it would seem entirely reasonable to have a biometric associated with an important document, such as a passport, in order to verify that the document is being presented by the rightful owner. However, this can be achieved with the biometric never leaving the passport. There is no need to construct databases and exchange biometric data with third parties in order to realise the benefits to passport agencies. Hence, clarity of purpose. If the purpose is to reduce document fraud, then this may be achieved in a simple and elegant manner.

Similarly, many would consider it acceptable for social services claimants to be issued with a local government card or token containing a biometric, in order that they may verify their identity at the service point of presence. Again, there would be no need to share this data with anyone else or have it leave the token. The biometric and associated personal data would be under the direct control of the individual.

There may be other possible applications where a user may wish to hold such a token for specific purposes, such as physical or logical access control. Once again, such a token may be specific to this purpose, under the control of the individual user and not associated with any database.

There are no doubt many such potentially positive applications. The common thread should be an absolute clarity of purpose, coupled to an operational methodology which places the

individual in complete control of their own data and how it should be used. In this way, identity management could come to mean something quite different to the current perception of the term. It is perhaps surprising that government agencies and technology suppliers alike, do not seem to have recognised how easily a different approach to identity management could make a huge difference from the societal perspective.

Conclusions and recommendations

The current focus upon identity management and the globalisation of identity management is somewhat bizarre. It is out of all proportion to the claimed benefits and clearly politically inspired. This is somewhat distressing to see, particularly within European Union member states who, typically, one would like to think would adopt a more societally sympathetic stance. Proposals are consequently being rushed through without proper debate, without an understanding of the societal implications and without reference to an agreed longer term strategy. We have to acknowledge the reality of this situation, before we can take steps to improve upon it. The problem is we have an 'emperors new clothes' syndrome, whereby there are few who are prepared to stand up and take an objective view of things, and even fewer who are prepared to listen. This situation must change if we are to avoid the more negative associations of identity management.

In this context, the author offers some recommendations for identity management within the European Union as outlined below:

1. Place an immediate freeze on projects of a national and international scale, and initiate a complete reappraisal of their objectives, costings and true benefits to society.
2. In parallel to (1) above, develop a unified longer term strategy which clearly sets out roles and responsibilities as well as defined objectives.
3. Develop an international awareness and associated strategy which protects the interests of European citizens.
4. Develop an identity management project methodology and associated template which ensures the right parameters are taken fully into account and that each such project has a 'clarity of purpose' statement, including risks, costs, and overall objectives.
5. Ensure that all related proposals are subject to full and open public discussion, requiring a majority approval before such proposals may be implemented.
6. Where a biometric and identity token is used, ensure that this token is under the full control of the user. If an enrolment database is used to guard against multiple enrolments by the same individual, then this should be a stand alone database with no third party connection or access of any kind.
7. Where user participation in any such scheme has ended, ensure that all associated personal data is erased from the system.
8. Ensure that sympathetic exception handling processes are in place for every initiative featuring identity management.
9. Ensure a complete in-house technical understanding around the use of biometrics and the importance of equivalence within every administration.
10. Publish a series of technical guidelines with special respect to identity management for the use of government agencies within the European Union.
11. Prohibit third party (especially private sector) involvement in the running of any public sector identity management initiative.
12. Prohibit the exchange of personal information with respect to any public sector initiative, unless imperative from a law enforcement or emergency perspective.
13. Establish a robust and secure mechanism whereby citizens may easily check what data is held about them by any government agency.

14. Prohibit the use of personal information resulting from a given initiative for any purpose other than that expressly stated within the terms of reference of that same initiative.
15. Prohibit the transference of resulting personal information to any agency outside the country of issue, without express permission of the individual, unless genuinely warranted in the interests of national or international security..
16. Embark upon an awareness campaign (within each applicable administration) in order to communicate the longer term strategy to citizens and receive feedback accordingly.
17. Establish proper training facilities for those public sector employees who will be involved with initiatives featuring identity management.
18. Set technological targets for future supporting technologies.
19. Establish an identity management senior council in Europe in order to monitor future related activity, both within the European Union and beyond and advise individual member states accordingly.
20. Support the development and usage of standards where applicable and highlight areas where additional standards might be beneficial.
21. Establish a Europe wide citizens advice centre for identity management issues, where claims around the mis-use of such data may be investigated.

There are many other such recommendations one could make, but the above perhaps serve to illustrate the current areas of weakness. It is perhaps worth reiterating that something as fundamentally important as public sector identity management, should be firmly under the jurisdiction of government, with government taking full responsibility accordingly. The current situation of government being largely advised by technology suppliers and government policy being shaped accordingly, is not an acceptable one. Especially from the longer term perspective.

Lastly, we have a broader and very important responsibility here, both to contemporary citizens and their descendants. Initiatives currently being established will set a pattern for a long time to come. We are creating a world for our children, and their children, to inherit and work within. We must strive to ensure that our rich European heritage is maintained, along with an acceptable quality of life which, in turn, provides the opportunity for individuals to realise a life of fulfilment within their chosen endeavours. It is the restriction of such qualities which leads to disenchantment and, eventually, civil strife. These are vitally important issues which we must understand and take fully into consideration with respect to the development of tomorrow's Europe. It is nothing less than our duty to do so. Identity management cuts right across these fundamental issues and, as such, is of prime importance. Currently, this importance is not reflected in the manner in which related initiatives are being proposed and pursued. We can change this.

Annexe

Societal Reconciliation

One of the important premises of the main body of this document is that technology alone cannot be expected to solve social and cultural issues: that is only achieved by understanding and intelligent policy. If we are to preserve the rich heritage of Europe, together with an attendant quality of life, for future Europeans regardless of their origin, then we must strive to reconcile the currently perceived cultural differences within and between the member states.

The situation has been accentuated by virtually uncontrolled mass migration into Europe from regions of widely disparate culture. Immigrants from such regions, unless particularly well educated, cannot be expected to fully understand the unique history and legacy of Europe. Conversely, indigenous Europeans are acutely aware of this history and its associated values, having fought two world wars in order to preserve the continuity of such values for future generations. Faced with the erosion of these values, together with overcrowding (particularly in the smaller member states) and diminishing resources, it is understandable that host populations will view mass migration into their beloved countries with suspicion.

It is no good to evade such issues, however difficult they may appear, nor to pretend that everything is fine. Everything is not fine. We have, in this Europe of ours, many millions of people who do not share the same values, understanding of history, or aspirations for the future. We have, in short, huge blocks of population who simply do not understand one another. The folly of forcing all of these people together within a finite space and resource quotient is a matter for future historians to ponder. However, the reality of mass migration is irreversible and its legacy will be that future generations will be growing up without the sense of identity and belonging which has, in the past, spurred so many Europeans to great achievements for both themselves and mankind in general. If we allow this situation to develop unchecked, we shall not only be rendering a disservice to future generations, but we shall be betraying our immediate ancestors and everything they worked, fought and died for. Surely, we cannot remain silent in the face of such a prospect, but must have the courage and conviction to work together in order to bring a resolution to current difficulties.

An appropriate starting point may lie in the acknowledgement that future generations borne in Europe will be Europeans, regardless of their ethnic and cultural roots. It is important that they feel European, speak European languages and have a burning desire to absorb and continue European values and achievements for the benefit of subsequent generations. Those borne to non-indigenous families will struggle to do this if they are not specifically taught these values and the European history that produced them. This needs to be a pre-requisite at every level of education. Furthermore, all members of future generations must be recognised and treated as Europeans: not as individuals of host or immigrant heritage. They must be subject to the same laws and the same opportunities.

To date, the practice in Europe has been to attempt to maintain parallel and disparate cultures within the same communities. This is a mistake. A very serious mistake, as all history shows, with regard to the continuity of values and civilisation. We must have the courage to acknowledge and rectify this mistake, for the sake of all Europeans, if we are not to lose forever the distinctions and noble achievements of these lands. This can only be achieved in the form of sympathetic and intelligent action. Action to reform policies and establish sustainable communities which work as one and offer hope for all. In this context the current situation is simply not sustainable.

There are two obvious threads which might usefully be pursued. The first is to immediately reform immigration and asylum legislation in order to halt the currently uncontrolled flow of migration into Europe. The smaller European member states are already suffering a crisis of proportionality in this respect, and if prompt action is not taken this will undoubtedly result in civil strife. The second is to reform education at all levels in order to both raise standards and, in particular, celebrate the history of Europe and instil a sense of pride in being European and continuing the rich thread of European culture. This can only be achieved by focusing upon the host culture and sharing its individual qualities and achievements with incoming citizens. It will never be achieved by trying to force foreign and disparate cultures into a host nation education system, as is currently being attempted in certain member states. The host culture must prevail if we are to ensure a peaceful and noble transition into a future Europe, wherein individuals of all backgrounds may feel at home and able to contribute to the common good within a framework of acceptance and brotherhood.

In order to pursue these threads and bring about the changes necessary to secure the future of Europe for all of its children, we must establish a plan of action. A roadmap from which we shall not be diverted by reasons of political or commercial expediency, but to which we shall hold true, in the face of whatever difficulties arise, for the benefit of those Europeans as yet unborn.

Conventional politics have so far failed to produce such a plan or, indeed, to even acknowledge the urgent need for one. This no doubt is in part due to the fear of being branded racist if one even considers the problem. We must not allow ourselves to be paralysed by this fear, but instead must find a way to highlight this omission and set the wheels rolling towards a more intelligent understanding accordingly. Moreover, in this quest, we should acknowledge the very special part that Europe plays in relation to the world. If this part is substantially diminished, it will have repercussions throughout this world, impacting the way of life for all human kind. The danger of it being so diminished is very real if we insist on pursuing current policies.

The above highlights the absurdity of proposing, or believing, that technology can solve societal problems. It cannot. Such problems may only be successfully addressed by intelligent policy. Technology may serve to support such policy in a carefully defined manner, but it is the policy that must come first: not the technology. The current paranoia and focus upon terrorism stems directly from poor policy, not a lack of technology. It is poor policy which is overcrowding Europe. It is poor policy which is threatening the environment. It is poor policy which is creating new economic pressures. It is poor policy which is creating energy monopolies. It is poor policy that is causing sky high serious crime rates. It is poor policy which is undermining healthcare. We must have the courage to address policy. We must not hide behind technology. Doing so creates an illusion of civilisation which is destined to be cruelly shattered, as surely as night follows day.

Julian Ashbourn

July 2006