LIBERTY AND SECURITY

STRIKING THE RIGHT BALANCE

PAPER BY THE UK PRESIDENCY OF THE EUROPEAN UNION

INTRODUCTION

The European Union has helped create freedoms for our citizens that were unimaginable 50 years ago. We can work and travel more easily than ever before, buy and sell over the internet with confidence and send money across borders at the click of a button. Yet despite this fantastic record many of our citizens remain highly sceptical about the European Union.

I believe that a deep reason for these doubts is that the European Union does not appear to give sufficient priority to offering practical solutions which make a difference to some of the issues of greatest concern. I refer specifically to serious and organised crime, including drug-dealing and people trafficking; to illegal migration and false seeking of asylum; and to countering terrorism whatever its origins. These issues top the political agenda across Europe, and they are often the most potent in mobilising political activity, often in a reactionary and even dangerous way.

I therefore believe that the whole European Union, but in particular the Justice and Home Affairs Council, needs to give real priority to tackling these issues in a practical and systematic way.

And in so doing I suggest three principle approaches.

The first is that in our globalised world no single country can tackle these problems alone, even in their own country. In each of these areas we will all, including within our own countries, achieve most by sharing experience, information and resources and by identifying, and then targeting, the threats systematically and consistently.

The second principle that must underlie our approach is to strengthen the foundation of practical and pragmatic police and intelligence work. In each of these areas we have already taken action at the EU level. For example we have agreed the European Arrest Warrant, common rules on the penalties and definitions for terrorism, people trafficking and other serious crimes. We have rules on police and judicial cooperation and have established Europol and Eurojust to support their work. We have also strengthened freedom to travel with the EU and established the European Borders Agency.

There is of course more that we can and are doing. We have agreed a comprehensive programme of action in the Hague Programme and the Counter-Terrorism Action Plan. These contain many sensible practical measures that will make a real difference to our citizens. If we want to demonstrate the real value of the EU we now need to work together to deliver on those commitments.

But it is the third principle which I believe poses the greatest challenge in its modern application. That principle is that we need to use intelligence effectively and intelligently to target, track down, identify and convict the criminals who through terrorist violence and committing serious and organised crime threaten the security and strength of our society.

Criminals and terrorists use modern technology: the internet and mobile communications to plan and carry out their activities. We can only effectively contest them if we know what they are communicating. Without that knowledge we are fighting them with both hands tied behind our backs. And

of course the criminals know that and actively and consciously organise themselves to take advantage of our weaknesses.

It may seem obvious to state in this way that we need to collect and use intelligence against the threats that we face. But this European Parliament, as well as national Parliaments throughout Europe, needs to face up to the fact that the legal framework within which we currently operate makes the collection and use of this intelligence very difficult and in some cases impossible.

The rules that currently govern our law-enforcement bodies seriously inhibit their ability to protect us against criminals. Information is the life-blood of law-enforcement operations and enables our police and agencies to prevent crimes with the minimum of impact on our daily lives. To tackle organised crime and to stop terrorist groups before they carry out activities they need a clear picture of who the criminals are, what they are doing, where they are and how they communicate with each other. Often that picture is pieced together after the fact. But if we are to be effective in dismantling organised crime groups we must analyse intelligence and information so that we can target our efforts on the most dangerous criminals. However, that need is not always reflected in the rules that we apply to our police.

This is not a sterile debate about principles but about practical measures to contest criminality and out opponents.

That is why we argue that internationally consistent and coherent biometric data should be an automatic part of our visas, passports and identity cards where we have them – and would even suggest driving licences as well.

I accept that in considering proposals in these areas it is incumbent upon the advocates of change, such as the British Government, to make the case that measures of this kind do have the practical advantages against criminality that I believe that they do. That is why I am publishing this paper on proposals being taken at EU and national level in particular those relating to retention of telecommunications data. I hope that the Parliament will look closely at the case that we put forward.

But I believe that the central point for us to remember is that as we make our considerations we should not forget that we now possess many hard-fought rights such as the right to privacy, the right to property, the right to free speech and the right to life. Those rights are actively threatened by criminals and terrorists. We have a duty and responsibility to help protect them for our citizens through practical measures. As we consider how best to do this there will always and inevitably be a balance in rights. What matters in each case is that the steps are proportionate and that protections against abuse are effective. I believe that our proposals offer that.

Charles Clarke

Retention of telecommunications traffic data

Summary

- Retained communication data has been crucial in unravelling terrorist networks and solving serious crimes.
- That will remain the case because terrorists and serious criminals have little choice but to communicate by phone or internet.
- In the UK, over half of all data requirements in terrorist investigations are for data over six months old.
- Only data generated or processed for business purposes is retained, so the extra cost for business is associated solely with keeping data for longer than it otherwise would be.
- The UK experience is that these costs are modest: £875 000 for one major mobile network.
- In the case of the internet, the requirement is to retain information about log-ins and log-outs alone.

Mobile phones and e-mails have a central role in the daily lives of people in the EU. For many of us they are indispensable tools in life. Sadly, the same is true for criminals. However, the technology that makes it easier for them to carry out their criminality can also be their downfall. The information that is automatically generated when they use their phones, mobiles and the internet can be as useful to those investigating crime as the physical DNA or fingerprints that can be left at the crime scene. Of course, it can also be used to corroborate alibis. In the UK it is an essential tool for investigating serious crime and is being used to find those behind the bomb attacks in London.

What is it?

Communications traffic data is the information that is generated automatically when their services are used; including information about where on a network a communication originates or terminates, the devices through which the communication is made and received and about the time the communication is made.

The service providers need this information themselves for legitimate business reasons enabling communications and managing their networks, for fraud detection and revenue collection. They currently keep differing sorts of data for different lengths of time. For example, information required simply for enabling the communication is not required by the provider immediately; data about network management is needed a little longer; and for fraud detection and revenue collection longer still. The periods of time that the information is kept for these purposes varies from provider to provider as they

are all currently deleted as soon as they have outgrown that provider's business need. An example of the data collected is attached to this paper.

How is it used?

Communications data can assist an enquiry by providing a link between people, times and places which may lead to the identification of witnesses, forensic opportunities or the criminal's financial assets. Drug and people traffickers conduct much of their business through the use of communication services and there are instances when mobile telephones have been used to detonate bombs. The ability to trace to whom a phone is registered, what calls were made, when and where they were made, whether answered or unanswered, means investigators can establish or refute certain events leading to a crime and the individuals associated with it. Terrorists and many serious criminals have already been brought to justice in the UK and other countries with the help of retained data.

In Sweden, a bomb threat was made to police by e-mail that a bomb had been placed at Stockholm Central Station. Using logs of the allocation of IP addresses retained by an Internet Service Provider, the source of the e-mail was traced to a public library in Stockholm. The library staff was able to provide information to the police that enabled the identification of the offender.

Why do we need a European model?

Most people acknowledge that in our globalised world cross-border crime is more prevalent than before. All of us agree that greater international co-operation is needed to tackle the problem.

However, as explained above, even within countries different service providers retain data for different lengths of time and so the ability of law enforcement to investigate serious crime is determined by the business practices of the particular service provider that a suspect, victim or witness of crime happens to use or have used.

And with different practices across the EU this element of chance is magnified even further. We are still in the relatively early stages of the investigation into the London bombings but it is clear already that there are international links that may lead to those who encouraged and supported the attacks. Fortunately Italy retains this information for as long as the UK does but should we really have to rely on chance?

In at least one case in the UK, the ability of the police and intelligence agencies to identify a terrorist network on the basis of an initial lead has depended on access to retained telecommunications data which revealed links between individuals otherwise invisible to investigators.

The draft Framework Decision would provide a legal basis for retention of specified data for the purpose of investigation, detection and prosecution of crime and terrorism. It would provide clarity for the telecommunications providers, law enforcement and safeguards for the public.

In the UK a suspect was eliminated from a murder investigation with unsuccessful call data. He gave evidence that he did not know the victim was dead and had, in fact been, calling her all day. His mobile phone call records showed no calls to the victim (because no calls to her had incurred a charge). The mobile phone company did not keep a record of connected-unanswered calls.

However because calls from a mobile to a landline will pass via the cheapest route, they can be present on another provider's interconnectivity records, which incur a charge (from one provider to another) and thus a record is generated. Communications data evidence showed 27 connected-unanswered calls between the suspects's mobile and the victim's landline, corroborating the man's explanation and eliminating him from enquiries.

Proportionality

In the UK telecommunications data is used to investigate serious crimes. IT is also only used proportionally. Law-enforcement targets their requests for access to data as required by the investigation. For example initially they may only ask for data collected on the day or in the vicinity of a murder. In the case of a terrorist attack they will seek a larger amount of data for a bigger area. In each case the request must be proportionate to the investigation. This is however only possible if the data is retained by the service provider.

Why 12 months?

Concerns have been expressed that retaining data for 12 months or longer is excessive. But data is often needed that is over 6 months old. Examples from Ireland make clear that data that is significantly older is sometimes used. A recent study of the requirements for disclosure of data made by the police in the UK established that the majority of data required (85%) was less than six months old. However, where data between 7 and 12 months old was required, it was used to investigate the most serious crimes, mostly murder.

That is for two reasons: firstly, the nature of the crimes may mean that the culprits do more to conceal their tracks so a crime (and therefore a suspect) may not come to light for weeks or months – for example where a dead body is only found months after a murder has taken place. In such circumstances investigators need to be able to look back in time to establish with who that victim may have been in contact at the time of death.

Secondly, in such crimes there will always be an expectation that such investigations will exhaust every line of enquiry and will run for longer, and that the acquisition of older data will be proportionate to the aim of detecting such offences.

In 2002 an aggravated burglary took place in a UK city. Over the following months similar offences occurred across the same city.

In each instance the victims were elderly single people or couples, who were tied up, assaulted and robbed of cash, valuables and credit cards. As the series of offences progressed the investigators wanted to determine if any mobile phone could be identified as being in the vicinity of more than one of the offences. This line of enquiry was rejected three times by the senior investigating officer as disproportionate to the offences then under investigation.

The victim of the ninth burglary died three months after being assaulted. By the time of her death at least fourteen offences were linked together and an offence of manslaughter was being investigated. This made the investigation of mobile phone location data and the acquisition of private communications data more proportionate to the aim of detecting the offenders.

Mobile phone data was obtained which proved links between the offences. Because data from the time of the earliest burglaries had been deleted evidence of the full extent of the criminality was lost. Several arrests have been made.

Why isn't intercepting their telecommunications sufficient?

Interception of telecommunications plays a very important part in tackling crime in the United Kingdom. However, it relies on suspicion in advance of a criminal act. It is entirely possible, with all the resources the UK has put in to tackling terrorism, for people who are completely unknown to the authorities to commit the most heinous acts. In other crimes there may be very little pre-meditation before the crime.

Won't they use other means of communicating

In the future some criminals and terrorists will adapt their use of technology to make the retention of this data a less important tool for investigators. However, with the current level of communications technology, this data is a necessary part of many investigations as it is difficult for terrorists and criminals to communicate without using the telephone or internet.

Costs

Experience in the UK and Ireland is that the costs associated with the retention of communications data are not excessive. For example, in its biggest project to date the UK Government is working with a national mobile phone network which represents a substantial share of the UK market and which presently retains all of its traffic data for two days. This data has a high degree of detail which can be valuable to investigators and includes outgoing and incoming answered and unanswered calls together with details of the geographical location of mobile equipment. After two days some of the data is retained for billing purposes and some is normally destroyed.

Following discussion with the UK Government the mobile phone network is proposing to retain all the data for 12 months. The total cost of doing so and providing a tool to retrieve specific data is £875,000 (€1.2m) and the UK Government is funding this project.

A Ghanaian national whose family owned what was described as a 'gold-field' came to London to sell a sample of gold. His contacts decided not to buy. The Ghanaian then went to the Netherlands for the same purpose. He was kidnapped, apparently at Schipol Airport, and a ransom demand was made to his family in Ghana, in the sum of £500,000.

The family reported the ransom to police in Ghana who contacted the UK police. The UK and Dutch authorities co-operated with the investigation. After four days there had been no contact from the hostage for more than 24 hours and the UK police were contacted to help identify the hostage's London contact. With the hostage's life at risk it was proportionate to seek relevant traffic data and the UK police identified a high frequency of calls from a hotel payphone to a Belgian mobile and to the family of the hostage in Ghana.

The Belgian mobile belonged to those guarding the hostage. Enquiries led the Belgian authorities to the place where the hostage was being held. He was rescued, having suffered severe torture. Arrests were made in Liege and in London.

For such a significant source of evidence these costs are not considered excessive for government or law-enforcement when set against other costs involved in pursuing criminals or terrorists.

In the UK our police can and do pay for communications data. In a typical murder case they may spend approx £50,000 (€72 400) on communications data, this rises to approx £500,000 (€724 000) for a terrorist investigation. This is a relatively small amount of their law enforcement budget and is not expensive when compared to other costs such as forensics: in a murder case forensics can exceed £500,000 (€724 000) and to forensically examine one cigarette end will cost the police approx £800 (€1158).

Internet data

We recognise the difficulty of retaining large amounts of internet traffic data and it is not the aim of the Framework Decision to require industry to retain this data. The Framework Decision only requires industry to retain information on when and where an individual logs-on and logs off the internet which will require substantially fewer resources.

Zero data calls

Unconnected calls are not included within the scope of the Framework Decision. Connected but unanswered calls are included within the scope because these can be signals to accomplices or used as a way of detonating explosives. The data call record attached shows some unconnected calls.

Data Protection

The UK understands the data protection concerns around this issue and there is absolutely no doubt that when data is retained by a service provider it must be stored securely.

Under the Framework Decision neither the police nor any public authority will have unrestricted access to the retained data. This will be governed by national law. Of course, they will only be permitted access for the reasons set out Framework Decision in the Directive, namely the investigation, detection and prosecution of crime.

Rules on access are regulated at a national level and police and other authorities will therefore have to meet the national standards to access private information.

The Presidency agrees that further clarity on the data protection rules relating to the third pillar would be helpful and we look forward to the Commission producing a proposal on data protection in the third pillar later this year.

EXAMPLE OF A TELECOMMUNICATIONS CALL DATA RECORD

Data Outgoing (Including Voice/SMS & Video Calls) for 078***975 for the period of 01/10/04 - 08/12/04**

Date & Time Of Call	Calling MSISDN	Called MSISDN	37 = Video Call	If populated with SMSC details then denotes SMS message)	Record Type	Duration In Seconds
19/11/2004 11:10	78*****975	**********			Mobile Originated	21
19/11/2004 11:11	78*****975	**********			Mobile Originated	3
19/11/2004 11:12	78*****975	**********			Mobile Originated	147
19/11/2004 11:39	78*****975	**********			Unsuccessful Call Attempt	
19/11/2004 11:39	78*****975	**********			Mobile Originated	181
19/11/2004 11:43	78*****975	**********			Mobile Originated	28
19/11/2004 11:44	78*****975	**********			Mobile Originated	1
19/11/2004 11:44	78*****975	**********			Mobile Originated	2
19/11/2004 11:45	78*****975	**********			Mobile Originated	390
19/11/2004 11:51	78*****975	**********			Mobile Originated	82
19/11/2004 11:53	78*****975	**********			Unsuccessful Call Attempt	
19/11/2004 11:54	78*****975	**********			Mobile Originated	0
19/11/2004 11:59	78*****975	**********			Unsuccessful Call Attempt	
19/11/2004 11:59	78*****975	**********			Mobile Originated	240
19/11/2004 13:42	78*****975	**********			Mobile Originated	34
19/11/2004 13:56	78*****975	**********			Mobile Originated	4
19/11/2004 13:56	78*****975	**********			Unsuccessful Call Attempt	
19/11/2004 13:58	78*****975	**********			Mobile Originated	91
19/11/2004 14:03	78*****975	**********			Mobile Originated	174
19/11/2004 15:08	78*****975	**********			Mobile Originated	6
19/11/2004 15:09	78*****975	**********			Mobile Originated	246

Biometrics in identity cards and passports

Summary

- Biometrics provide an improved method of linking a document and person and of checking someone's identity against a database. They are being increasingly used in the commercial sector.
- The EU is committed to making use of biometrics in passports and visas. This will improve the ability to identify multiple applications.
- ID cards are used for travel in the EU. Member States should look to greater use of biometrics in ID cards.

Moving between countries and travel across borders has always required people to prove their identity and their right to travel and to stay. This is the purpose of an identity card, passport or visa. In a globalised world in which people can move and travel more easily than ever before we need to devise more effective ways of confirming identity. In the 20th century this meant adding a photograph to passports, in the 21st century this means using biometrics, which are now acknowledged as being the most reliable way of establishing identity: far more effective than identifying a person by associated information such as his name, date of birth or through a person making a visual comparison with a photograph.

Biometrics confirm the identity of an individual by measuring the subject person's physiological features. They provide a way for a person to verify their identity by making a comparison of their biometric information with that stored in a chip on a document or on a database, thus preventing people using multiple different identities.

To turn our backs on proven biometric technology, to ignore the use made of fingerprints, iris and digital photos by both government and the private sector would be to reject the twenty-first century. Technical advances cannot be uninvented, nor should we wish to do it. We should bear in mind that the world of commerce, particularly the financial sector, has embraced biometric technology to regulate access to premises and facilities. If we are to offer our citizens a high degree of security we should do so too.

Types of biometrics

The biometrics chosen by the International Civil Aviation Organization are facial, fingerprint and iris pattern. Facial is the mandatory biometric and fingerprint and iris are optional secondary biometrics. The EU regulations relating to biometrics in travel document, visas and residence permits specify facial and fingerprints as the biometric identifiers.

Current plans are to use facial images for verifying identity by comparing the image stored on the document with the document holder in what is known as a one to one match. Fingerprints can also be used in this way i.e. they can be stored on a document (passport or visa) and electronically compared with the

fingerprint of the document holder. Given the long experience in using fingerprints they are robust, reliable, accurate and quick. This means that they can also be used for identification by checking and individual against the biometric records of others in a database in what is know as one to many matching.

Lastly there is iris. There is no provision at present to make use of iris recognition as a technology but in early trials it has been demonstrated to be highly effective. For example this is being used at Schipol airport and by businesses.

> *On 28 March 2004 a visa was issued to a Tanzanian applicant who was a frequent traveller to the UK. His wife, an employee of Oman Air, was due to accompany him on the trip. A fingerprint match then revealed that he had claimed asylum as a Somali national during a previous visit to the UK. The applicant and his wife were called into the British High Commission and re-interviewed in light of the fingerprint information. Their visas were revoked.*

Storage

Biometric data can either be recorded on a chip (for biometric passports and residence permits), or a database (for visas). For the purposes of a passport, the data will be stored in a chip on the passport and protected from unauthorized access by an access control. For residence permits, the data will be stored in a chip on a separate card. Again, this chip will be protected from unauthorized access.

It is however more secure to save biometric information to a database. This removes any possibility of false data being inserted on the chip by third parties. The delay in accessing data on a chip because of the security controls means comparison with a database is faster. However all parties wishing to verify identity need access to such a database and this solution is currently only viable at EU level with Visas through the Visa Information System.

The need for biometrics in Identity Cards

At EU level ID cards are often used to demonstrate a right to travel. For that reason Member States believe it is important that their national identity cards are secure, and have some common security features, ensuring a degree of consistency. Although, the EC does not have legislative competence in this field there would be advantages in setting minimum security and technical standards.

The inclusion of biometrics in identity cards will significantly improve the effectiveness and efficiency of proving identity when using an identity card. For example it will be possible to prevent people, particularly criminals, enrolling on a given system twice, because their biometrics can be checked against those already on the database: so it will not be possible to have multiple ID cards. It also means a person can better prove their established identity when using public services or in commercial transactions. The term "established identity" is used because, although the biometric is important in making a link to a person, it has to be combined with reliable checks on an individual's actual identity.

For its planned identity cards the UK is considering biometrics which are compliant with ICAO (International Civil Aviation Organisation) standards on machine readable documents. This means images of ten fingerprints, both irises and a digital photograph. In this form biometrics provide a very powerful tool: a recent study found that in principle fingerprint or iris recognition can provide the performance required to uniquely identify the entire UK adult population. This means that it will make it harder for individuals to fraudulently claim rights e.g. to travel, to access services. This will help to prevent criminals or terrorist groups from impacting on society as a whole through their activities. It will also help reduce the growing incidence of identity theft by fraudsters which recent research in the UK has shown to be the public's most significant anticipated benefit.

During a trial the majority of participants strongly agreed that biometrics do not infringe civil liberties and showed an overwhelmingly positive attitude towards the use of biometrics. The data collected will be subject to the UK's Data Protection Act 1998 and the Human Rights Act 1998 both of which bring into UK law the Data Protection Directive and the ECHR respectively. A new post of National Identity Scheme Commissioner will be created and will provide independent oversight of the way in which the scheme is administered. The UK legislation will not give the police any new powers in asking for, or in checking, someone's identity. It will also specifically rule out making the carrying of a card compulsory.

We believe that a card scheme open to everyone who is in the country over 3 months and which treats everyone on an equal basis will help to reduce discrimination, as everyone will have an equal means of proving their identity when using public services. The scheme will also help many people who now find it difficult to prove their identity in routine commercial transactions and in accessing services. A significant number of people in the UK do not have bank accounts, passports or driving licences and can feel excluded from much of mainstream society. They will be eligible for an identity card, which will give them all they need to demonstrate their identity.

A modern border control: using passenger name records

Summary

- Ever greater numbers of people travel across the EU's borders bringing benefits to the EU. We also use borders to improve security for our citizens and visitors.

- Passenger Name Records represent information collected for commercial purposes for flight segments of a journey but can also provide vital clues for law-enforcement.

- By building up profiles indicating engagement in criminal activity it is possible to focus law-enforcement efforts on the highest risk. This is carried out in a proportionate targeted way.

The challenge

By 2010, it is anticipated that some 120 million people will travel to the UK each year. The numbers for the European Union as a whole are significantly greater. The International Organisation for Migration estimate that there are 175 million international migrants worldwide (a figure which has more than doubled over the last 35 years) and Europe is a major host area for them.

No country wants to deter the legitimate business travellers who are critical to their economy. At the same time we rely heavily on an effective border control in our counter terrorism strategies, in tackling organised criminal activity as well as maintaining an immigration control. In carrying out our border control work we must strike the balance between legitimate trade and travel, processed with the minimum of inconvenience, against the harm caused by organised crime.

Against the background of increased travel and greater internal freedoms countries must find ways for our border agencies to work together more effectively to protect our borders. Increasingly countries are turning to an intelligence-led approach to border management.

Proper risk analysis and intelligence-focussed border management by law enforcement agencies, underpinned by access to passenger information in advance of travel, can support a more effective and flexible control that is appropriate to the perceived level of threat at any given time. In particular it allows law enforcement resources to be focussed where they are most needed and provide the potential for faster processing of low-risk passengers

Passenger Name Records

A Passenger Name Record (PNR) in the air transport industry is the generic name given to records created by aircraft operators or their authorised agents for each journey booked on or behalf of any passenger. The data is used by operators for their own commercial and operational purposes in providing air transportation services. A PNR is built up from data that has been supplied by or on behalf of a passenger concerning all the flight segments of a journey.

This data may be added to by the operator or authorised agent, for example changes to requested seating, additional services required, etc. The structure of individual PNRs and the amount of data they contain vary widely. The number and nature of the fields of information in a PNR will vary depending on the reservation system used during the initial booking, or other data collection mechanism employed, the itinerary involved and also upon the special requirements of the passenger. PNR data comprises a range of elements such as date of ticket reservation, date and place of ticket issue, payment details, passenger/travel agent contact details and travel itinerary. An example of a PNR is attached at Annex A.

Police Officers investigating a rape in London held a suspect who claimed to be out of the UK at the time of the alleged offence. Examination of flight manifests and PNR data allowed police officers to quickly disprove his alibi.

How is it used?

PNRs are particular important in the intelligence-led approach to border control. They can provide law enforcement with a valuable source of data for risk assessment and intelligence purposes. Through a combination of operational experience, specific intelligence and historical analysis the border agencies can build up pictures of suspect passengers or patterns of travel behaviour. PNR data may then be used to indicate suspect behaviour by enabling the identification of individuals whose travel details share common characteristics with those pre-defined profiles.

Indicators or profiles can be of varying degrees of complexity. For example, operational experience may indicate that tickets used by a number of passengers who arrived undocumented were purchased with a single credit card. This indicates that the credit card may be linked with facilitation. The identification of the same payment details in a future booking will be, therefore, of significant interest to the Immigration Service. Whilst a single reservation data element can identify an individual of interest, it is more usually a combination of elements which indicate a suspect passenger and constitute a profile (e.g. a ticket purchased with cash at a 'suspect' travel agency). It is also important to emphasise that profiles would not be set in stone. They are in a constant state of flux and may differ from region to region, route to route and carrier to carrier.

The UK Immigration Service has successfully used PNR data to disrupt the facilitation of inadequately documented passengers. In August 2005, PNR checks on the basis of known profiles and a particular travel agency revealed six suspicious bookings on flights from Barcelona to Heathrow and Gatwick. The Heathrow Intelligence Unit informed the Airline Liaison Officer in Madrid who alerted the airline. As a consequence, the six passengers were identified as using counterfeit passports and were arrested by the Spanish police after being denied boarding.

Given that the value of passenger information is not confined to a single journey it is essential that law enforcement and intelligence agencies can retain PNR for a sufficient period of time as is necessary to achieve the aim of maintaining an effective border security capability. In the national security

context, experience has taught that during the investigation following a terrorist incident the ability to historically identify suspected perpetrators by reference to their travel is a vital investigative tool. As the terrorists may have entered the country a considerable time before the incident the retention of the data for a reasonable of time is therefore necessary. We see this as a fundamental building block for enhancing border security

Striking the right balance

In taking forward work on Passenger Name Records in the EU and with our international partners it will be important to clearly define what we mean by PNR as well as being clear about the purposes for which PNR may be used by Member States. The EU Commission are in the process of developing a proposal for the use of PNR and, indicative of their support for the initiative, Member State, including the UK, Germany, Spain, France and Italy, are participating in that work. In addition, there are extensive discussions in the ICAO on the issue with a view to establishing a recommended practice.

In the UK for example, Customs authorities have been using reservation data as a fundamental element of their intelligence-led control for some time. They can point to significant successes as a result of targeting based on the use of such information, for example, at London Airports a relatively small group of staff undertaking profiling with PNR data accounting for 30% of seizures of prohibited and restricted items.

Of particular importance in ensuring public confidence in the activities of the law-enforcement agencies is that data protection and Human Rights are respected. This means that use of the data elements contained within PNR which a carrier may be required to provide to MS should be in compliance with provisions under Directive 95/46/EC and equivalent national legislation, such as the Data Protection Act 1998. For example in the UK the authorities have to show that it is necessary and proportionate to hold data for a particular period and that data is not being retained for longer than needed. In any given case proposals must strike the right balance between protecting the privacy of the individual and ensuring that the Border Agencies have the capability to exercise fully their border security functions, removing barriers to effective operation wherever necessary.

A key aim of the UK e-Borders programme is to co-ordinate and enhance the existing levels of access that the border agencies variously have to PNR data. This will involve the establishment of processes to safeguard data and to ensure that it is used in a manner which is consistent with the border agencies' data protection obligations. As part of that work, the e-Borders Programme is engaging with the Office of the Information Commissioner who is responsible for ensuring compliance with the Data Protection Act 1998.

EXAMPLE OF A PASSENGER NAME RECORD

Description	Example
Fare (TST) Indicator	--- TST RLR---
Header Line	RP/LONXX0940/LONXX0940 OC/PR 12SEP01/1402Z X4NOQ7
Received from	RF MRSTANLEY
1,2,3 – Name	1. STANLEY/SAMMR 2. STANLEY/DONNAMRS 3. STANLEY/DEAN (CHD)
4 – Itinerary	4 XX 949 C 02MAR 6 MUCLHR HK3 1135 1235 *1A/E*
5 – Itinerary	5 XX 954 C 10AR 7 LHRMUC HK3 1725 2010 *1A/E*
6 – MCO	6 MCO XX MUC 02MAR/GBP 150.00/*CAR RENTAL/P1
7 – Contact	7 AP MUC 089 975 654123 – H
8,9 – Ticketing arrangements	8 TK OK12SEP/LONXX0940
	9 TK PAX OK12SEP/LONXX0940/ /ETXX/S4-5/P1-2
10,11 - Seat requests (Psgr 1 seat 4D, Psgr 2 Seat 4E, Psgr 3 seat 4F non smoking)	10 SSR RQST XX HK3 MUCLHR/04DN:P1/04EN:P2/04FN:P3/S4
	11 SSR RQST XX HK3 LHRMUC/09FN: P1/09JN: P2/09KN: P3/S5
12, 13 – Meal requests	12 SSR RQST XX HK1/S4/P2
	13 SSR RQST XX HK1/S5/P2
14 – OSI	14 OSI YY 1CHD/P3
15 – Confidential Option	15 OP LONXX0940/12SEP/X – 02FEB/CONFIDENTIAL OPTION
16 – General remarks	16 RM GENERAL REMARK – CAN BE READ BY ALL AMADEUS USERS
17 – Corporate Remarks	17 RX CORPORATE REMARK – CAN BE READ BY ALL XX OFFICES
18, 19, 20 – FA (ticket numbers)	18 FA PAX 125-2100000007/GBP418.50/12SEP01/LONXX0940/91496716/S4 -5/P3
	19 FA PAX 125-2400500020/ETXX/GBP612.50/12SEP01/LONXX0940/91496716/S4- 5/P1
	20 FA PAX 125-2400500021/ETXX/GBP612.50/12SEP01/LONXX0940/91496716/S4- 5/P2
21, 22, 23 – FB	21 FB PAX 1000000066 TTP/PT/XH1 OK PROCESSED/S4-5/P3

	22 FB PAX 1000000070 TTP/ET/XH1 OK ETICKET/S4-5/P1
	23 FB PAX 1000000071 TTP/ET/XH1 OK ETICKET/S4-5/P2
24, 25, -FE Endorsement	24 FE *M* NO CASH REFUND/P1
	25 FE *M* REFER REFUND SELLING OFFICE/P2
26, 27 – FP Forms of Payment	26 FP CCA549983000000049/0203/N5311/P1

CLOSED CIRCUIT TV

Summary

- CCTV is widespread and has little impact on the daily lives of citizens. However, it can prove critical in identifying criminal activity after the fact.
- While it is used in a many locations the number of images recorded, viewed or ever used is small. The use and collection of images is also subject to data protection laws.

The CCTV images of the 7 July London bombers brought to the attention of law enforcement across Europe the assistance that such footage can provide in the search for and identification of criminals and terrorists. As shown by this example, CCTV can be important in identifying those who have committed crimes and helping police, with public assistance, to identify and bring offenders to justice. It can also have an impact on reducing crime, especially tackling certain types of premeditated crime (e.g. vehicle crime). But public concerns over the balance between their privacy and the use of CCTV footage need to be met.

The Soho Bomber: in April 1999 a device exploded in a pub and three people died and 65 were injured. The offender was identified as a result of CCTV evidence. It was also used to track his movements through central London.

CCTV can be used in a wide range of locations, including car parks, town and city centres, residential areas, and even on public transport systems. It is more successful where cameras have extensive coverage, and are focused on entrances and exits to key areas. It is important that research is carried out in parallel to the use of CCTV to assess its overall impact and to determine in which circumstances CCTV could have the greatest impact on crime and on public fears. Research has shown that members of the public were less likely to worry about being a victim of crime in those areas with CCTV.

Is it proportionate?

It is difficult to accurately say how much CCTV material is ever used by or in connection with law enforcement. However, it is estimated that less than half of CCTV pictures are ever viewed by law enforcement officers, a smaller percentage is actually recorded and an even smaller amount is ever retained for any length of time. It would be unusual for recorded material to be retained for any length of time except where it is specifically required in connection with an investigation.

In 1993, a two year old boy was abducted from a shopping centre near Liverpool by two ten-year olds and tortured to death. CCTV evidence suggested to the Investigating Officers that the abductors were children not adults, which would have been a more natural assumption.

In order for CCTV to be effective, the aims and objectives of CCTV need to be clear in terms of what problems and issues it seeks to address. Schemes must be properly managed, supported by relevant technical experts. There needs to be a clear and informed decision making process on where to place cameras and consideration on the type of camera used, ensuring that it is 'fit for purpose'. Control room operations are extremely important in using CCTV to help detect crime.

Data Protection

In order to ensure that CCTV footage is used fairly and lawfully, it is important that CCTV operators comply with data protection principles. In processing personal data, it is useful to require those handling this data to comply with a set of enforceable principles of good data handling practice.

Conclusion

This paper has looked at four practical developments both in the EU and at national level that have the potential to increase the security of our citizens. They also raise difficult questions about the balance between our various rights. The UK Presidency is committed to taking forward the debate with its partners on these and other issues. The Presidency is open to answers questions that MEPs may have.