Passenger Information

Latest Update

26th February 2015

Author

David Lowe – Liverpool John Moores University

Introduction

With the current terrorist threat facing European Union Member States, including the UK coming from those citizens joining terrorist groups such as Islamic state and the Al Qaeda affiliate Jabhat al-Nusra Front in Syria, Iraq and Libya, with that threat being of serious concern on their return to the home state it is vital that national security and counter-terrorism policing agencies have access to detailed flight information. While many states already have access to Advanced Passenger Indexes (API),as this article will show the information is limited. In 2011 the European Union introduced a draft directive regarding the exchange of passenger name record (PNR) but due to concerns over data protection and rights to privacy this directive was not introduced. As seen with the Paris attacks in January 2015 and the attack in Copenhagen in February 2015, the terrorist threat that was present in 2011 has changed. This article will examine the difference in API and PNR information and argue why a PNR Directive is needed in the current climate.

Overview of the Topic

1. ***The EU's Directive on Passenger Name Records 2011/0023-*** *Information contained in Passenger Name Records Data.* In February 2011 the European Commission produced a proposal for a directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2011/0023). At the time of its publication the explanation memorandum covered issues as to why the directive was needed by agencies involved

in investigating terrorism and serious crime where a comparison was drawn between PNR and aircraft passenger information (API). PNR's contain the following information:

1. Name of Passenger;
2. Contact details for the travel agent or airline office;
3. Ticketing details;
4. Itinerary of at least one segment, which must be the same for all passengers listed;
5. Name of person providing the information or making the booking;
6. Passenger gender;
7. Passport details (includes nationality, passport number and date of passport expiry);
8. Date and place of birth;
9. Billing information;
10. Form of payment (include debit/credit card details);
11. Contact details (potentially include landline/mobile phone numbers);
12. Frequent flyer data; and
13. Vendor remarks kept by the airline (International Civil Aviation Organisation (2010) Guidelines on Passenger Name Record (PNR) Data Quebec: International Civil Aviation organisation).

This is far more extensive information compared to API's that only contains a passenger's name, date of birth, gender, nationality and passport details and this limitation was recognised by the European Commission in the explanatory memorandum to the PNR Directive saying:

> 'API data does not enable law enforcement authorities to conduct an assessment of passengers and therefore do not facilitate the detection of hitherto "unknown" criminals or *terrorists*' [my emphasis] (2011/0023 Directive p.7).

While API is useful in terrorism investigations at port and border controls for investigating officers to ascertain who is on a flight list that can be checked to suspects already contained within intelligence systems, the point being made above is API's are restrictive when trying to ascertain the identity of those who are not known. However the additional information contained in the Directive such as who made the booking or contact details and methods of payment can be cross-checked to see if there is a connection with terrorist suspect in intelligence systems. As stated above, Europol have already found that there are groups facilitating the travel of individuals who may referred to in intelligence circles as clean-skins, that is they are not on any intelligence system. However if from the PNR data a link is made,

this will greatly assist the officer in agencies investigating terrorism. The fact that PNR data is an important intelligence tool is also recognised in the PNR Directive's explanatory memorandum (Directive 2011/0023 Explanatory Memorandum p.8).

2. ***Key Provisions in the 2011 PNR Directive*** **-** While clearly stating the scope of use of PNR data was the prevention, detection and prevention of terrorist offences and serious crime (Directive 2011/0023 article 9) the Directive recommended that Member States identified competent authorities to process the PNR data issued form Passenger Information Units (Directive 2011/0023, article 5). It is clear that no decision should be taken by the competent authority on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life. One concern with the Directive related to data retention was the protection of personal data and the transfer of data to third countries. In essence, the proposed period of detention of data by competent authority was 30 days, with the Passenger Information Unit to retain the data for 5 years (Directive 2011/0023 article 9). The protection of the data should be covered by the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (FD 2008/977/JHA). The data subject has the right to expect the competent authority to fulfil their duties regarding their duties under the Framework Decision (article 18) and that includes the right for the data subject to have a judicial remedy for any breach of the rights guaranteed to them by the applicable national law (FD 2008/997/JHA article 20). Where the PNR data is transferred to a third country the Framework Decision makes it clear that it has to be ensured that the third country had an adequate level of protection of the intended data processing (FD 2008/997/JHA article 14).

3. ***Concerns Regarding The PNR Directive*** **-** The European Parliament expressed concerns that the proposed method of automatically processing PNR data using fact based pre-determined assessment criteria was very wide and thought that such an assessment should never result in , '…profiling on the basis of sensitive data' (Directive 2011/0023 Memorandum p.10). In light of current issues regarding terrorist groups such as Islamic State, compared to when the PNR Directive was proposed the terrorist threat has escalated in severity since 2011 and is not only real but is potentially dangerous to the right to life of EU citizens. This is important as the European Data Protection Supervisor also questioned if the PNR Directive was necessary and proportionate, with the main concern being the collection of data of innocent persons. He criticised the Directive proposal as contributing towards a surveillance society (Directive 2011/0023 Memorandum p.10).

4. ***Concerns Over a Surveillance Society*** **-** In April 2013, the Committee on Civil Liberties of the European Parliament (LIBE) saw the PNR Directive being too wide and consequently refused to agree for the need of the Directive. The concerns mainly cantered on Passenger Information Unit as having the potential to refuse to erase a person's data even if they are not suspected of a crime and the Committee had a concern the Directive left it open to authorities to carry out offender profiling on individuals who matched certain behaviour (The European Citizen 2014). 2013 was a year where fears of a surveillance society were confirmed following the revelations by the former US National Security Agency (NSA) employee, Edward Snowdon on the practices of the NSA and the UK's General Communications Headquarters (GCHQ) in particular Operation PRISM and the bulk surveillance of electronic forms of communication and telephone use, some of which was unauthorised (Greenwald 2014 pp.33-42). The shock waves of the NSA's actions reverberated around the world,

more so when it was revealed that politicians in the EU's Member States were also spied on by the NSA, in particular the German Chancellor Angela Merkel (Greenwald 2014 p. 141). As Greenwald (the *Guardian* newspaper journalist Snowden passed the NSA documentation onto) says, what is more remarkable are the revelations that the NSA was spying on millions of European Citizen adding;

> '…in addition to foreign leaders the United states … also spied extensively on international organisations such as the United Nations to gain a diplomatic advantage.' (Greenwald 2014 p142)

It is understandable why there is such a concern in recommending further powers of surveillance to national security and policing agencies, yet a balance has to be drawn between the needs of protecting the interests of security within the EU's Member States and the rights of individual citizens.

European Union law is clear that personal data is to be protected. Article 16 of the Treaty on the Functioning of the European Union (TFEU) states that everyone has the right to the protection of personal data concerning them (TFEU C326/55 Article 16(1)) and the European Parliament and the Council must act in accordance with ordinary legislative procedure that will lay down rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, office and agencies when carrying out activities that fall with the scope of EU law (TFEU article 16(2)) as does article 39 in the Treaty of Union. The Charter of Fundamental Rights of the European Union also is clear that everyone has the right to the protection of personal data concerning them (2000/C 364/01 Article 8(1)) 8(2)). In that right it states, '…data must be processed fairly for specified purposes on the basis of consent of the person concerned *or some other legitimate basis laid down by law'* (2000/C 364/01 Article 8(2)) [My emphasis]. This is in addition to the respect the state must have for the right of a person to their private and family life in both the Charter of Fundamental Rights of the European Union (2000/C 364/01 Article 7) and the Council of

Europe's European Convention of Human Rights (ECHR) (Article 8). Article 8 of the ECHR does allow for the state to interfere with the right to privacy where it is under an act proscribed by law and it is necessary in democratic state when it is in the interests of national security or to prevent crime or disorder.

These projections are upheld in the agreements the European Union has with the United States regarding the transfer of PNR (Agreement between the United States of America and the European Union on the use and transfer of Passenger Name records to the United States Department of Homeland Security 17434/11) and the agreement with Australia of PNR data (Agreement between the European Union and Australia on the processing and transfer of Passenger name records (PNR) data by air carriers to the Australian Customs and Border Protection Service 10093/11). In the agreement between the US and the EU it states the US will confirm that effective administrative, civil and criminal enforcement measures are available under US law for privacy incidents and the US Department of Homeland Security will take disciplinary action against persons responsible for inappropriate use of the privacy conditions (17434/11 article 5(6)). It also says in the agreement that the Department of Homeland Security will inform the relevant EU authorities of cases of privacy incidents involving PNR of EU citizens (17434/11 article 5(4)). Similar provisions relating to data security and integrity also are present in the agreement between the EU and Australia (10093/11 article 9) including the separate storing of EU citizens' PNR data and it is only stored for the purpose of matching with intelligence data Australian authorities have on persons suspected of being involved in terrorism or serious crime (10093/11 article 9(1)(a)). The EU has understandably taken a strict approach as to how intelligence and citizens' personal data is handled and dealt with by state authorities as provided in the European Commission's overview of information management (Communication from the Commission

to the European Parliament and Council: Overview of information management in the area of freedom, security and justice COM(2010)385 final) which concludes saying:

> 'Adopting … a principled approach to policy development and evaluation is expected to enhance the coherence and effectiveness of current and future instruments in a manner that fully respects fundamental rights.' (Communication from the Commission to the European Parliament and Council: Overview of information management in the area of freedom, security and justice COM(2010)385 final, p.28)

This is seen in the current Directive regarding the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences (Directive of the European Parliament and of the Council on the protection of individuals data 2012/0010 (COD)) that is expected to be introduced in 2016.

5. ***New EU Data Protection Regulation and Directive*** **-** The EU was looking to amend the data protection provisions it currently has in place prior to the Snowden revelations, however the EU is looking to introduce changes to take effect by 2016 at the latest that will tighten up EU citizens' data protection, in particular regarding data exchange with third countries. The two pieces of legislation proposed are:

1. Personal data protection regulation: processing and free movement of data (General Data Protection Regulation) 2012/0011 COD;
2. Personal data protection directive: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties and free movement of data, 2012/0010 COD

The regulation will have an impact in the private sector as businesses will have to set up new processes to facilitate the rights of citizens to access information held on them. Regarding the directive the transfer of data to a third country/international organisation will only occur if it is for the same purpose as the directive and that organisation is a public authority in a state that provides a proper level of data protection within a country where appropriate safeguards are established in a legally binding instrument (article 33).

Post the January 2015 terrorism events in Europe, the EU's Justice and Home Affairs Commission has brought back on the EU's legislative agenda a proposal for blanket coalition and storage of passenger name record data for up to five years on all records of passengers flying in and out of Europe. It is not a given that the plans will become legislation in the EU as the vice-chairman of the European Parliament's civil liberties committee, Jan Philip Albrecht sees the plans as an affront, in particular to the EU's main court, the European Court of Justice decision in *Google Spain SL, Google Inc. v Agencia Espanola de Prrteccion de Datos (APED)* Case C-131/12, which held in 2014 that data retention without any link to risk or suspicion is not proportionate. For Albrecht a plan to blanketly retain all passenger data would be open to a breach of fundamental rights would be open to a breach of fundamental rights (Travis 2015).

6. ***A Proposed New Version of a PNR Directive*** **-** While the Directive 2012/0010 (COD) is expansive in its coverage of criminal activity it is submitted that a separate directive is required to deal with the transfer of PNR. andBuilding on the 2011 draft PNR Directive, a new draft text on an EU system for the use of PNR data was tabled by lead Member of the European Parliament (MEP), Timothy Kirkhope (ECR, UK) that was discussed in the LIBE Committee on 26 February 2015. An evaluation of the necessity and proportionality of the proposal in the face of current security threats, its scope (list of offences covered), retention periods, the inclusion or exclusion of intra-EU flights, the connection with the on-going data protection reform, as well as the consequences of the EU Court of Justice judgement annulling the 2006 data retention directive, were among the issues discussed by MEPs. The 2011 Commission proposal would require more systematic collection, use and retention of PNR data on passengers taking "international" flights (those entering the EU from, or leaving it for,

a third country), and would therefore have an impact on the rights to privacy and data protection.

The changes proposed by Timothy Kirkhope in the revised draft report include:

1. The scope of the proposal is narrowed to cover terror offences and serious "transnational" crime (the list of specific offences includes, for instance, trafficking in human beings, child pornography, trafficking in weapons, munitions and explosives);

2. Sensitive data to be permanently deleted no later than 30 days from the last receipt of PNR containing such data by competent authorities. Other data will continue to be masked after 30 days;

3. The inclusion of intra-EU flights (not initially included by the Commission, but the Council of the European Union favours the inclusion of internal EU flights);

4. 100% coverage of flights (the Commission text proposed to reach 100% coverage of international flights in gradual steps);

5. Access to the PNR data continues to be allowed for five years for terrorism, but is reduced to four years for serious crime;

6. Each EU member state should appoint a data protection supervisory officer;

7. Persons who operate security controls, who access and analyse the PNR data, and operate the data logs, must be security cleared, and security trained;

8. References are made in the text to the EU Court of Justice judgment on data retention and to the current EU data protection rules; and,

9. The period for member states to transpose the directive is extended from two to three years (given the specific technological and structural demands of setting up an EU PNR system for each member state).

In addition to Kirkhope's it is submitted that consideration be given to the following points:

1. Any amended Directive is solely related to terrorism investigations;
2. The Directive only applies to targeted flights to and from states that border or are terrorist conflict zones;
3. The PNR data is only held by competent authorities (who would be Member States' national security agencies and Counter-Terrorism Policing Departments);
4. Requests for PNR data on applicable flights is carried out through and by Europol on behalf of the respective Member State competent authority requesting the data;
5. It is necessary that all Member States collect, process and exchange PNR data to avoid security gaps as this will contribute towards the security of the EU;
6. All PNR data is handled in accordance with the provisions of Article 8 of the Charter of Fundamental Rights of the European Union, Article 16 of the Treaty on the

Functioning of the European Union and article 39 treaty for Union along with article 8 ECHR;

7. The data is pulled from the PNR data solely for matching purposes in relation to terrorism intelligence already in the possession of the Member States' competent authorities. The data cannot be requested for sole purpose offender profiling, thereby preventing data mining.

In addition to these suggestions, the sections referring to serious crime is omitted and by targeting terrorist conflict zones this reduces the concern over data mining by Member States' competent authorities. The main aim of counter-terrorism investigations is to prevent terrorist acts from happening and ensuring that EU Member States' citizens are safe. Such a proposal would enhance this capability.

Key Acts

None

Key Subordinate Legislation

European Convention on Human Rights

Key Quasi-legislation

None

Key European Union Legislation

Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data 2012/0010 (COD)

Directive on Passenger Name Records 2011/0023

Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters FD 2008/977/JHA

The Charter of Fundamental Rights of the European Union 2000/C 364/01

Treaty of the European Union 1992

Treaty on the Functioning of the European Union TFEU C326/55

Key Cases

Google Spain SL, Google Inc. v Agencia Espanola de Prrteccion de Datos (APED) Case C-131/12

Key Texts

Agreement between the United States of America and the European Union on the use and transfer of Passenger Name records to the United States Department of Homeland Security 17434/11

Agreement between the European Union and Australia on the processing and transfer of Passenger name records (PNR) data by air carriers to the Australian Customs and Border Protection Service 10093/11

Communication from the Commission to the European Parliament and Council: Overview of information management in the area of freedom, security and justice COM(2010)385 final

Further Reading

Greenwald, Glenn (2014) *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State* New York: Metropolitan Books

The European Citizen (2014) 'Draft EU PNR Directive voted down at Committee Stage' retrieved from http://theeuropeancitizen.blogspot.co.uk/2013/04/draft-eu-pnr-directive-voted-down-at.html [accessed 7th September 2014]

International Civil Aviation Organisation (2010) Guidelines on Passenger Name Record (PNR) Data Quebec: International Civil Aviation organisation

Travis, Alan (2015) 'European counter-terror plan involves blanket collection of passengers' data' *The Guardian* 28th January 2015 retrieved from http://www.theguardian.com/uk-news/2015/jan/28/european-commission-blanket-collection-passenger-data [accessed 28th January 2015]