Passenger Name Records: a Tool to Fight Terrorism across Europe

By Richard Ashworth MEP

A more interconnected world is a better world and global travel brings with it countless possibilities. Yet, this greater freedom also provides opportunities for those who wish to do us harm. The European Union (EU) provides a framework for Member States to coordinate their actions in the fight against terrorism and organised crime; successful examples include the European Arrest Warrant which allows for extradition of suspects across the EU, whilst the European Criminal Records Information System permits judges and policemen to access criminal records across the Union. To further protect citizens from potential attacks, the European Parliament has just voted for the Passenger Name Records (PNR) report, steered through the Parliament by British Conservative MEP, Timothy Kirkhope.

Passenger Name Record data is already collected by airlines, but this new European Union legislation sets out detailed rules for national authorities to access it when tackling serious crime. It allows for the transfer of basic passenger information given at the time of booking a flight in the EU to identify patterns of suspicious behaviour.

So what is PNR?

Passenger Name Record data is routinely collected for commercial purposes, and includes names, contact details, itinerary, and the credit card used for payment and baggage information. Passport details are collected through Advance Passenger Information. The system is used already in the USA and UK to detect terrorist activity, drug and people trafficking. The data collected has proven valuable to highly-trained analysts, and the agreement will allow all data to be collected on all flights into and out of the EU, as well as flights within the EU as well.

What about privacy and sovereignty?

EU Member States will collect and process PNR data on travel under an agreed legal framework to help protect citizens from harm. The data will be retained for a maximum of five years so that law enforcement officials can access it if necessary. Data cannot be processed that reveals a person's race or ethnic origin, religion, political opinion, trade union membership, health or sexual life.

The UK does not have to participate in EU Justice and Home Affairs policies. The government decided to be involved this time because the UK already has its own system of e-Borders including PNR.

So why is it so important?

The serious crimes covered by the new legislation include terrorism; trafficking in drugs, people or weapons; cybercrime; and sexual exploitation of children. PNR data has a proven capability to protect our citizens from harm. During 2005-2011 the UK's e-Borders system has led to over 1,500 people being refused entry and over 8,700 arrests; including 57 for murder, 175 for rape/sexual assault, 397 for drugs offences and 920 for violence.

PNR data had already helped to thwart terrorist attacks. For example, it was instrumental in capturing collaborators of the 7 July 2005 London bombers and of David Headley, the terrorist facilitator convicted in the US of involvement in the Mumbai attacks in 2008.

By collecting, sharing and analysing PNR information our intelligence agencies can detect patterns of suspicious behaviour. PNR is not a silver bullet, but we face a real threat of foreign fighters returning from Syria and other war zones. Modern criminality requires modern methods to seek out and shut down criminal activity. We cannot just focus on solving crimes after they have happened. Instead we must use the tools available to prevent them happening in the first place. The EU PNR Directive is good for our safety, good for our security and good for citizens: it will make a Britain safer place.

To contact Richard Ashworth MEP:
Email: richard.ashworth@europarl.europa.eu
Website: http://www.richardashworth.org
Twitter : @RichardAshMEP