Hard Brexit, soft data: How to keep Britain plugged into EU databases

by Camino Mortera-Martinez

23 June 2017

Retaining full access to EU databases fighting crime and terrorism will not be easy for Britain. Any deal will require a role for the European Court of Justice and keeping EU privacy laws.

On June 7th, four days after the London Bridge terrorist attack which left eight dead and 48 injured, it emerged that the Italian authorities had warned their British counterparts about one of the perpetrators, Italian citizen Youssef Zaghba. His details were uploaded to the Schengen Information System (SIS), an EU-wide law enforcement database, after he was stopped at Bologna airport while trying to reach Syria. It is unclear precisely what information was put into the system – the British authorities claim that the SIS alert only suggested that Zaghba was involved in a non-terrorism related crime. But Zaghba's case is just the latest proof of the importance of EU co-operation on counter-terrorism. It will remain so after Brexit.

EU databases are crucial if this co-operation is to be successful. The British government knows this, and will therefore try to retain access after the UK leaves the EU. But if Theresa May insists that Britain will not be subject to the jurisdiction of the European Court of Justice (ECJ), things may turn out much more difficult than she expects.

There are three areas of particular importance for European co-operation against crime and terrorism. In decreasing order of difficulty in the Brexit negotiations, these are the European Arrest Warrant (EAW); access to databases such as the Schengen Information System; and police and judicial co-operation through the EU agencies Europol and Eurojust. In none of these areas is Britain likely to retain the same status it enjoys now. But in most of them, the EU and the UK will be able to reach an agreement that keeps the UK as closely associated as possible. This will require a bit of creativity.

This insight is the second in a three part series, and looks at whether or not the UK will be able to remain plugged into the EU's law enforcement databases, and, if so, under what conditions.

Over the past 20 years, the EU has built a vast array of databases (see table below). Every database serves a different purpose, from catching criminals to gathering information on visa applications. Each has one or more different legal bases, depending on its purpose: if one part of a database is used for law enforcement, and another to secure Schengen's external borders, that means different legal bases. In normal times this would be a simple technicality. But it matters for post-Brexit Britain because its negotiating leverage for retaining access to a Schengen database is not the same as for remaining part of a database containing information on air passengers. Because the UK is not part of the EU's passport-free Schengen travel area, it may be more difficult for the British government to convince the EU to give Britain full access to Schengen databases than to those with a different legal basis.

Exclusive Schengen databases: The Schengen Information System

Britain is not, and has never been, a member of Schengen. Despite being an outsider, the UK was given partial access to Schengen's main law enforcement database, the Schengen Information System – a database storing data on wanted and suspicious people – but only after a fight. It took the UK several years to connect to SIS: the database only went live in Britain two years ago. Some member-states thought a non-Schengen country should not have access to a database created to protect the Schengen area. Britain only has access to the law enforcement part of SIS, not the border control part. London cannot, for example, input or receive data on irregular migrants who have been removed from the EU.

After spending £39 million plugging the UK into SIS, the British government would like to continue using it post-Brexit. The government's own Brexit white paper underlines the value of SIS, observing that "from April 2015 to April 2016, over 6,400 foreign alerts received hits in the UK, allowing UK enforcement agencies to take appropriate action, whilst over 6,600 UK-issued alerts received hits across Europe".

But negotiating access to SIS will not be easy. There may be an EU-wide consensus on keeping Britain as closely involved in European security measures as possible, but some technical problems will still need to be resolved. There is no legal basis in the EU treaties for a non-EU, non-Schengen country to participate in Schengen. Countries like Australia or Canada can only obtain SIS information by asking Europol to run a search for them. In 2010, the UK asked for access to another Schengen database, the Visa Information System (VIS, containing fingerprints and digital photographs of those applying for a Schengen visa). The British government wanted access to VIS only for the purposes of fighting crime, but the European Court of Justice denied it, arguing that the UK was not part of Schengen and as such should not benefit from information stored in Schengen databases.

Life is easier for non-EU, Schengen countries, but still no bed of roses. Iceland, Norway and Switzerland all have access to SIS. But in exchange for their participation in Schengen, they must pay into the EU budget (in 2015 Norway paid €6 million to participate in EU justice and home affairs); they must also accept the supremacy of the ECJ over their national courts in matters related to Schengen. If the ECJ and Norwegian, Icelandic or Swiss courts disagree on the interpretation of one of their agreements with the EU, the agreement will be terminated. The three countries must also follow ECJ case law when incorporating any part of the Schengen *acquis* into their domestic law. Last but not least, non-EU countries must follow EU data protection standards if they want to access Schengen databases. Some of these non-EU Schengen countries may be unhappy if the EU offers the UK a similar deal to the one they enjoy. Schengen is no more popular in Bern than in London and Swiss politicians may have a hard time explaining to their voters the point of being in Schengen if an outsider can have access to Schengen databases but still maintain their own border controls.

Exclusive Schengen databases			
Name of database	**Scope**	**Purpose**	**Who can access it**
Schengen Information System (SIS)	Centralised EU database	Stores 'alerts' (information on people and objects), so that countries can: control people at borders, identify and detain criminals (including terrorists) and track persons of interest and stolen goods.	Full access: border guards, police bodies, custom officers and judges. Partial access: Europol, Eurojust, visa and migration authorities.
Visa Information System (VIS)	Centralised EU database	Stores fingerprints and digital photographs of those applying for a Schengen visa. Upon entry into the Schengen area, countries can check visa holders against the database, to verify their identity, detect potential fraud and fight against crime.	Full access: competent visa authorities and border guards. Partial access: asylum authorities, Europol, national bodies dealing with counterterrorism and third countries (in specific cases).
Non-exclusive and non-Schengen databases			
Eurodac	Centralised EU database	Stores fingerprints of asylum seekers, to determine the country responsible for their application. It can also be used for law enforcement purposes, to identify criminals.	Full access: asylum and migration authorities. Partial access: police.
Prüm databases	National databases, accessible to all EU countries	National databases storing DNA profiles, dactyloscopic data and certain national vehicle registration data. EU countries must make this data available to other member-states. They also must provide information in relation to major events, and to fight terrorism.	National law in each member-state determines who has access to this data. This can include police forces and security and intelligence agencies.
European Criminal Records Information System (ECRIS)	National databases, accessible to all EU countries	National databases storing information on criminal records for EU nationals committing crimes in countries other than their own.	National law in each member-state determines who has access to this data. This includes judicial authorities but may, in some cases, include others like prospective employers.
Passenger Name Records (PNR)	National databases, accessible to all EU countries	National databases storing information on air passengers, including name and address of the passenger, baggage information, banking data, itinerary and emergency contact details. It is used to investigate and prosecute serious crimes, including terrorism.	Full access: national authorities competent to detect, investigate and prosecute serious crimes.

Source: Centre for European Policy Studies and the Centre for European Reform's own research.

Britain will certainly not join Schengen after it leaves the EU. But if it wishes to continue exchanging information with Schengen countries, it will have to compromise on some of Theresa May's red lines, namely ECJ jurisdiction and paying into the EU budget. London will also need to comply with EU privacy standards.

Data protection will be all the more important in the case of Schengen databases because of the sensitivity of the information in them: to justify giving the UK a special status, the EU may demand that London not only retains EU privacy laws, but is also willing to allow the European Commission to scrutinise British data protection standards periodically. The EU may demand to know what exactly London is going to do with the data and with whom it plans to share it. The European Commission could issue an 'adequacy decision' (which certifies that a country's privacy standards are good enough for the EU), reviewed annually, to ensure that standards have not been lowered in Britain. In its 'adequacy decision', the Commission would not only look at British data protection laws, but also at legislation on national security (such as the UK's 'Data Retention and Investigatory Powers Act' -DRIPA), which also affect the transfer of SIS data to and from the UK. Given the EU's dislike of Britain's intelligence regulations – the ECJ said in 2016 that parts of DRIPA were illegal – and Brussels' suspicions of the UK's 'special relationship' with the US in intelligence, the EU will want to be reassured that Schengen data is always treated in a way it deems compatible with its stringent privacy standards.

Non-exclusive and non-Schengen databases

Negotiating access to non-exclusive and non-Schengen databases should be easier for the UK, provided it meets some requirements, including continuing to comply with EU data protection standards. If Britain wants to retain access to Eurodac (a database storing fingerprints of asylum seekers, which can be used both to determine in which country they made their application and for law-enforcement purposes), it will probably have to remain a part of the EU's Dublin asylum system. The Dublin system makes the country where asylum seekers first enter the EU responsible for looking after them (allowing member-states to send people back to Italy or Spain, for example). Staying in Dublin while leaving the EU may seem counter-intuitive, but it makes sense: the UK, as a member of the 1951 Geneva refugee convention, is obliged to take in refugees and forbidden to send them back to unsafe countries. It can send them back to safe countries, however. The UK is a net beneficiary of the system (in 2014, the last year for which data are available, the UK sent 252 asylum seekers to other member-states but received only 69), so it should have an interest in staying in, at least as an associate member.

Britain will also most probably seek access to the EU's Passenger Name Records (PNR) system, used for exchanging information about airline passengers departing for or arriving from third countries, and ECRIS, a database storing information on criminal records.

It should be fairly straightforward to negotiate an associate status for the UK, allowing it to participate in the EU PNR scheme. After all, Britain was behind the adoption of the system, and it already has all the necessary technical requirements in place. The British government should seek an associated status to the existing EU scheme, rather than risk going into an all-consuming negotiation on a separate EU-UK PNR agreement. The ECJ struck down an earlier PNR agreement with the US and is in the process of reviewing the agreement with Canada; the EU's advocate general has recommended that the Court overturns this one too.

The UK is the fourth largest user of ECRIS – in 2015, British requests for information through ECRIS disclosed 178 convictions for rape overseas and 177 murder convictions. There is no precedent for a non-EU country accessing ECRIS (not even non-EU Schengen countries do), but the British government could try to convince its EU counterparts of the added value of having Britain connected to the system.

Finally, the UK government will also try to stay plugged into the Prüm databases. These are national databases storing DNA profiles, fingerprints and certain national vehicle registration data, which must be made available to other member-states. There is a precedent for access to the Prüm databases by non-EU members: in 2009, the EU signed an agreement with Norway and Iceland granting them access.

After the UK's June 8th general election, in which Theresa May lost her parliamentary majority, nobody knows what kind of divorce from the EU Britain will seek. Theresa May's demand before the election was to end the European Court of Justice's jurisdiction over the UK. That would mean the UK losing some crucial information tools in fighting crime and terrorism. At a time when the UK government's Joint Terrorism Analysis Centre has assessed that the terrorist threat to the UK is 'severe', the Conservative party and its allies in power would do well to remember what they risk by being too dogmatic.

Camino Mortera-Martinez is a research fellow and Brussels representative at the Centre for European Reform.