

## EU-US cooperation in Justice and Home Affairs – an overview

### SUMMARY

The United States is the key partner of the European Union in the area of justice and home affairs (JHA), including in the fight against terrorism. While formal cooperation on JHA issues between the US and the EU goes back to the 1995 New Transatlantic Agenda, it is since 2001 in particular that cooperation has intensified. Today, and for the period up until 2020, the key areas of transatlantic efforts in the JHA field are personal data protection, counter-terrorism and countering violent extremism, migration and border controls, tracing of firearms and explosives, money laundering and terrorism financing, cybercrime, drugs and information exchange.

Regular dialogues at all levels, extensive operational cooperation and a series of legal agreements demonstrate the development of the transatlantic partnership on JHA. Assessments state that cooperation on law enforcement and counter-terrorism has led to hundreds of successful joint operations each year, and many foiled terrorist plots. Nevertheless, important challenges remain, in particular in light of the revelations of US mass surveillance activities and the resultant growth in EU concerns about US standards for data privacy.

The European Parliament is making use of its extended powers in the JHA field, by urging a high level of data protection as well as effective and non-discriminatory means of redress for EU citizens in the US over improper use of their personal data.



### In this briefing:

- Background
- Political dialogue on JHA and operational cooperation
- Priority areas
- EU-US legal agreements
- An assessment of transatlantic cooperation and remaining challenges
- The European Parliament
- Main references

## Background

Formal EU-US cooperation on justice and home affairs (JHA) [started](#) in 1995, on the basis of the [New Transatlantic Agenda](#) and the [Joint EU-US Action Plan](#), and was significantly reinforced after the 9/11 attacks.<sup>1</sup> In particular, [cooperation](#) on cross-border law enforcement and intelligence, including counter-terrorism, has been one of the EU's key priorities since 2001; today the relationship with the USA is the EU's most advanced in this area. In particular, EU-US cooperation has been focused on the fight against [terrorism](#) and transnational crime, law enforcement and information exchange for law enforcement, protection of personal data, border management, visa and migration policies, and cybersecurity and cybercrime.

The US has increasingly recognised the EU as an actor in its own right (rather than the Member States) in the JHA area. Regular high-level political and security dialogue, extensive contacts, inter-agency operational cooperation, as well as a series of legal agreements between the US and the EU are evidence of this recognition, and of the evolution of the transatlantic partnership on JHA matters. Nevertheless, despite the continued emphasis on shared values, significant [challenges](#) to cooperation remain due to the different EU and US approaches. The revelations of US mass surveillance programmes and intelligence collection in Europe have affected transatlantic trust, and intensified EU concerns about data privacy and information exchange on the other side of the Atlantic. Other tensions have arisen in respect of US detainee policies, differences in terrorist designation lists in the US and EU, as well as border control and security measures.

## Political dialogue on JHA and operational cooperation

The [political dialogue](#) on justice and home affairs issues, including counter-terrorism, is the EU's most advanced with any third country, considering the number and level of contacts and the extensive policy cooperation. These links between officials on both sides of the Atlantic have increased since 2001 and, today, EU-US meetings take place regularly at both ministerial and senior official level:

- Biannual ministerial meetings on justice and home affairs;
- Biannual JHA informal high-level meetings (normally at the start of each six-month EU Council presidency);
- Biannual political dialogues on terrorism between the US State Department and the European External Action Service (EEAS); and between the Commission and the US Department of Justice;<sup>2</sup>
- Biannual dialogue of legal advisers of the EU, Member States and the US State Department, on counter-terrorism and international law;
- Steering committee on countering violent extremism (several times a year);
- [Dialogue](#) on terrorist financing;
- High-level policy dialogue on border and transport security;
- EU-US [Working Group](#) on Cybercrime and Cybersecurity;
- Expert-level dialogue on protection of critical infrastructure.

EU-US cooperation at **operational level** is also highly [developed](#), and is now a [daily event](#) for internal security and intelligence agencies, judicial authorities, treasury and trade authorities, border security and transport authorities. Law enforcement agencies share data and intelligence, and conduct joint operations. For example, joint operations

in the counter-terrorism area have been run against identified terrorist networks, including coordinated freezing of financial assets and the surveillance and disruption of their means of online communication. According to Europol, in 2014 alone, more than 600 international operations were initiated in [cooperation with US federal agencies](#) leading to many operational successes in various crime areas, including against ['darknet' marketplaces](#), large-scale violation of [intellectual property rights](#), currency counterfeiting, cybercrime and organised crime groups involved in the distribution of child sexual exploitation material. Of a yearly average of 500 operations [initiated](#) in cooperation with the US, around 50 are considered high-impact operations.

The mutual exchange of liaison officers has also advanced inter-agency and operational cooperation: two Europol liaison officers are posted in Washington DC, while [US liaison officers](#) from 11 federal agencies are posted to Europol and a permanent liaison prosecutor works at Eurojust.

### Priority areas

In October 2009, EU and US ministers adopted the [Washington Statement](#) on enhancing transatlantic cooperation in the Area of Justice, Freedom and Security, which set out the principles and main areas of EU-US cooperation, such as mobility, law enforcement, counter-terrorism, judicial cooperation, fundamental freedoms, resilience and international cooperation for the following five years. The EU and US intended to build on the progress achieved up to that point (on customs cooperation, extradition and mutual assistance, passenger name records (PNR), and operational arrangements) and also take into account the EU's multiannual priorities in the Area of Freedom, Justice and Security under [the Stockholm Programme](#), adopted a few months later.

In June 2015, the EU-US ministerial meeting on Justice and Home Affairs [endorsed](#) the [Riga Statement](#) which reconfirms the principles of the Washington Statement, and outlines **new priority areas** for transatlantic cooperation during the next five years (as well as a set of concrete actions for each area): personal data protection, counter-terrorism and countering violent extremism (CVE), migration and border control, tracing of firearms and explosives, money laundering and terrorism financing, cybercrime, drugs and information exchange. In recent years, the threats from foreign terrorist fighters and organised crime have climbed high on the transatlantic [agenda](#), with measures such as border security, visas, and information exchange being discussed to address these threats. In addition, the current Dutch Council Presidency has set out its [priorities](#) in this area, namely migration and counter-terrorism, as well as a special focus on cybersecurity and cybercrime (as well as human trafficking, victims' rights and cooperation on forensic science).

### Counter-terrorism and countering violent extremism (CVE)

Since 2001, transatlantic cooperation in the fight against terrorism has intensified. A series of agreements aimed at increasing cooperation and information-sharing for the purpose of law enforcement, including countering terrorism (see section below), have been concluded between the US and the EU, in addition to the bilateral cooperation and arrangements in place between the US and individual Member States. Several joint Declarations and Statements on counter-terrorism have been issued over the years, including the 2010 [Declaration on counter-terrorism](#), whereby the EU, its Member States and the US announced their resolve to combat international terrorism within the rule of law, and set out the main areas and tools for cooperation in this respect. A specific joint [interest](#) has emerged in **radicalisation and countering violent extremism**

since 2008-2009, and this has [intensified](#) in recent years. The Steering Committee on CVE meets several times a year and discusses issues such as terrorist travel, countering terrorists' online activities, challenging extremist narratives, deradicalisation programmes in prisons, and cooperation on CVE activities in third countries. Inter-agency cooperation in this area has also developed between Europol and the US Department for Homeland Security (DHS); the US also recently [suggested](#) placing US agents in Europol to work on [counter-narratives](#) in the online environment. [Foreign terrorist fighters](#) has become a [priority](#) issue for EU-US counter-terrorism cooperation,<sup>3</sup> as well as addressing **terrorist financing**. Cooperation on border security, aviation security, intelligence and information-sharing between law enforcement agencies, and counter-radicalisation efforts have become interlinked issues in the EU and US fight against terrorism.

On the other hand, several [problematic](#) topics have affected transatlantic cooperation on counter-terrorism, including differences between EU and US designated terrorist lists, data protection, and the US practices of extraordinary rendition and secret detention facilities. In addition, there have been tensions related to the US visa-free travel arrangements ([Visa Waiver Program](#)) which are not applied uniformly to all EU citizens.

### **Personal data protection**

Despite the adoption in 2009 of [common personal data protection principles](#) by the US and the EU, personal data privacy continues to be one of the most important [challenges](#) in transatlantic cooperation, both with regard to the information-sharing agreements [for law enforcement purposes](#) – such as the EU-US Agreement on Passenger Name Records (PNR) and the TFTP/SWIFT agreement – and to the frameworks for commercial data transfers from the EU to US. Many in the EU, including the European Parliament, have raised serious concerns with regard to the [protection of personal data](#) in the US, claiming violations of EU citizens' basic rights. The 2013 Snowden [revelations](#) of mass surveillance [activities](#) in Europe by the US National Security Agency have reinforced EU demands for stronger levels of data protection in the US, as well as for non-discrimination for EU citizens with regard to the means of redress available in the US. In this context, [restoring trust](#) in the transatlantic relationship has been underpinned by the revision of existing agreements regulating data transfers and the negotiations of new ones, such as the Umbrella Agreement.

### **Migration and border security**

The EU and US have concluded several agreements on customs cooperation, including mutual recognition of air and maritime cargo security regimes. The US DHS also signed in 2009 a working [arrangement](#) with Frontex, the EU's agency for border management cooperation, covering areas including risk assessment, sharing of best practices, exchange of information, training, and joint operations.

As regards passenger travel, the issue of complete visa-free travel for EU citizens to the US has been one of the sticking points in transatlantic relations. The US Visa Waiver Program (VWP) is in place for 23 EU Member States, granting their citizens short-term visa-free travel to the US.<sup>4</sup> The VWP has recently been [modified](#) out of security concerns arising from the foreign fighter threat, a decision that raised serious concerns in the EU. Moreover, on a bilateral level, the US has sent official [requests](#) to five EU Member States to start negotiations on 'pre-clearance agreements', under which US Customs and Border Protection (CBP) officers deployed at the departure airport in the EU would

determine whether passengers and their baggage or goods headed to the US may be admitted into the country. Currently, (non-Schengen area member) Ireland is the only EU Member State that has [pre-clearance facilities](#) for passengers bound for the US, and these have been in place since 2009. While the UK reportedly welcomed the US request, other EU Member States such as Sweden and the Netherlands raised [concerns](#), principally related to whether the Schengen rules would allow such facilities, and over fundamental rights.

Moreover, the refugee crisis in the Mediterranean has pushed migration and refugee issues higher up the transatlantic agenda. Cooperation on migration issues continues in the framework of the EU-US Platform on Migration and Refugee issues, launched in 2010. The Platform's action plan includes priority [areas](#) such as return and reintegration, biometrics, resettlement, trafficking in human beings, migration management capacity-building and labour migration. More recently, the [possibility](#) of enhancing US political and operational [support](#) to the EU was analysed, including EU cooperation with the US military in the Mediterranean.

### **Cybersecurity and cybercrime**

In the area of [cybercrime and cybersecurity](#), EU-US cooperation started in 2010, when the parties also established the EU-US Working Group on Cybersecurity and Cybercrime (WGCC). The EU-US WGCC addresses four main areas: cyber incident management, private-public partnerships, including for critical infrastructure protection, the fight against cybercrime, and raising awareness on cybersecurity. In 2011, the first joint cyber exercise was held (Cyber Atlantic 2011), aimed at improving coordination and more accurately identifying vulnerabilities. In 2014, the [EU-US Cyber Dialogue](#) was put in place, expanding cooperation and with the aim of addressing cross-cutting cyber issues, international developments in this field and foreign-policy-related cyber issues.<sup>5</sup> The EU and US also cooperate in the framework of [Europol](#) and [Eurojust](#) on fighting cybercrime; a particular area for transatlantic cooperation is the fight against sexual abuse online, including the fight against [child sexual exploitation](#).

### **EU-US legal agreements**

The EU and US have concluded a series of binding agreements, including on arrangements for information sharing, on extradition and mutual legal assistance (MLA), on passenger name records (PNR), on container security, and on sharing financial data for the purpose of the US [Terrorist Finance Tracking Programme](#) (TFTP).<sup>6</sup>

#### **Agreements in the field of police and judicial cooperation, and information sharing**

##### *Extradition and mutual legal assistance*

In 2003, the EU and the US signed two treaties, on [extradition](#) and mutual legal assistance ([MLA](#)),<sup>7</sup> which entered into force in 2010. The EU-wide extradition agreement with the US is [considered](#) to modernise the existing bilateral extradition agreements between the US and Member States. It streamlines exchange of information and documents, and sets rules for establishing the priority in cases of competing extradition requests. Under Article 13 of the extradition agreement, the US agreed not to impose/execute the death penalty on suspects extradited from the EU.

MLA agreements establish cooperation for the purpose of gathering and exchanging information in judicial investigations, and assistance in obtaining evidence located in another country. This also entails requests by law enforcement authorities to assist each other in cross-border criminal investigations or proceedings. The US-EU MLA



agreement covers issues such as identification of bank information (providing US authorities with access to European financial information in criminal investigations), setting up joint investigative teams, video-conferencing, expedited transmission of requests, assistance to administrative authorities, use limitations, confidentiality, and grounds for refusal. The EU-US agreement does not replace the [bilateral US MLAs](#) with EU Member States (bilateral agreements are in force with all Member States except Bulgaria and Croatia), but supplements them.

#### *US agreements with Europol and Eurojust*

In 2001 and 2002 two **US-Europol agreements** were concluded which allow for the sharing of [strategic](#) and [personal information](#) in law enforcement. The negotiation of the agreement on personal information was particularly difficult, due to EU insistence that the agreement reflect EU standards on the protection of rights and rule of law. A **US-Eurojust cooperation agreement** was concluded in 2006. This was followed in 2007 by an EU-US [agreement](#) on the **security of classified information**, which sets some common standards so as to facilitate the exchange of classified information.

In February 2015, two other [agreements](#) were signed between Europol and US Customs, relating to foreign terrorist fighters and illegal immigration, issues now high on the agenda for cooperation. The first agreement [associates](#) the US CBP to Europol's [Focal Point Travellers](#), which is a tool created in 2013 for the collection, analysis and sharing of information related to the recruitment and travel of foreign terrorist fighters. The second agreement (Focal Point Check Point) aims at enhancing transatlantic cooperation against illegal immigration, targeting in particular organised crime groups that facilitate such immigration.

#### *Tracking terrorist financing: the SWIFT/TFTP agreement*

In August 2010, the US-EU [Agreement](#) on sharing **SWIFT** banking data (or financial messaging data) for the purpose of the US Treasury Department's **Terrorist Finance Tracking Program** (TFTP) entered into force for a period of five years. In August 2015, the TFTP/SWIFT Agreement was automatically renewed for a period of one year.

Under the TFTP agreement, the US Treasury Department [submits](#) a reasoned request for specific financial and banking data to the SWIFT company (Society for Worldwide Interbank Financial Telecommunication) located in Belgium. A copy of the request is sent to Europol, which ensures the request conforms with the provisions of the agreement. If validated by Europol, SWIFT is bound to comply with the request and provide the data to the US. Article 9 of the TFTP Agreement obliges the US to share any information obtained in the framework of the TFTP deemed useful for the EU and its Member States in the prevention or investigation of terrorism-related activities. Under its Article 10, the EU Member States, Europol and Eurojust can request the US Treasury Department to search for specific information in the SWIFT data.<sup>8</sup>

#### *Transfer of Passenger Name Records (PNR)*

Following 9/11, the US adopted legislation requiring air carriers to give the US DHS access to passengers' data prior to their flights' departure, both leaving from and heading to the US. The EU and the US signed an agreement in 2004 to provide a legal basis for the transfer of PNR data from the EU to the US, which was later invalidated by the EU Court of Justice. A new PNR agreement was [signed](#) in 2007, but amid concerns about the protection of data and judicial redress for EU citizens in the US, the European Parliament postponed giving its consent to the agreement, eventually endorsing the opening of new negotiations with the US, launched in December 2010. This latest EU-US

[agreement](#) on the use and transfer of PNR data to the US DHS 'for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and transnational crime'<sup>9</sup> entered into force in July 2012 for a period of seven years. In exchange, the agreement provides that the DHS will ensure an appropriate level of data security, and includes provisions on the protection of sensitive data, on retention periods, on transparency and individual access to PNR data, on correction and rectification requests, as well as (administrative) redress for individuals. The Commission considers the agreement to be a useful tool in fighting terrorism and transnational crime, while giving adequate safeguards for EU citizens' PNR data.

### Protection of personal data

#### *Safe Harbour and the new EU-US Privacy Shield agreement*

The purpose of the **Safe Harbour Framework** (2000) was to [protect](#) EU citizens' data if transferred to the US by American companies; it included a [self-certification mechanism](#) whereby US companies indicated their compliance with the Framework's principles on personal data. As a result, such companies were allowed to transfer data from EU Member States to servers based in the US. In October 2015, the Court of Justice of the EU (CJEU) [invalidated](#) the Commission's 2000 [decision](#) on the Safe Harbour arrangement which had recognised that the US ensured an adequate level of data protection, in accordance with European data protection legislation. The ECJ thus effectively ruled that the US [failed](#) this 'adequacy test'.<sup>10</sup>

The replacement for Safe Harbour – the EU-US [Privacy Shield](#) – was agreed on 2 February 2016. The **EU-US Privacy Shield** will form the new framework for transatlantic data flows and will consist of a Commission decision finding that the new protections, which the US government has promised to put in place, are adequate for preserving the privacy of citizens who provide their data to US companies. The Commission points out that the US has given the EU, for the first time, binding assurances that access by public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, while EU citizens will benefit from judicial redress mechanisms in this area. The Commission has published the [documents](#) pertaining to the new arrangement and is awaiting the [assessment](#) of the [Article 29 Data Protection Working Party](#). In the meantime, data transfers to the US should be based on [alternative legal frameworks](#) such as Standard Contractual Clauses and Binding Corporate Rules.

#### *The EU-US 'Umbrella Agreement' on data exchanges for law enforcement*

The EU-US ['Umbrella Agreement'](#) on data privacy and protection of data exchanged **for the purpose of law enforcement** was initialled in September 2015 ('for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters'). Its negotiation began in March 2011. A condition for the agreement to be signed and formalised was the enactment by the US of the [Judicial Redress Act](#) (JRA), amending the 1974 US Privacy Act in response to EU demands for equal rights of access to civil remedies in the US for EU citizens concerning their personal data. The JRA was passed by the US Congress on 12 February 2016 and signed by the President on 24 February. This new legislation allows the US Department of Justice to designate foreign countries, or regional economic integration organisations, enabling their citizens to bring civil actions under the 1974 Privacy Act against certain US government agencies for the purpose of accessing, amending, or redressing unlawful disclosures of records

transferred to the US in the framework of law enforcement. The JRA is also of relevance for the Privacy Shield agreement for data transfers for commercial purposes.

The Umbrella Agreement is intended to [provide](#) an overarching framework of rules governing transatlantic data exchange in the context of law enforcement investigations, and set high standards of personal data protection for future agreements in this field. However, the Umbrella Agreement will not provide a legal basis for actual transfers of data, which will still require the conclusion of specific agreements. To conclude the agreement, the Council has to adopt a decision on the basis of a Commission proposal and following the consent of the EP. However, the European Data Protection Supervisor proposed several changes to the text in a preliminary [opinion](#) on the Agreement. Furthermore, some [Members](#) of the European Parliament and the EP's [Legal Service](#) have raised concerns about the agreement's compatibility with primary EU law and fundamental rights.

### **Border controls and transport security**

#### *The EU-US air cargo security agreement*

In June 2012, the Commission and the US Transportation Security Administration (TSA) signed a mutual recognition [agreement](#) of each other's **air cargo security regimes**. It is meant to speed up transatlantic shipments and reduce costs for US and European cargo shippers. EU-US cooperation to strengthen border controls and transport security also played an important role in getting other states to agree the 2010 [International Civil Aviation Organization declaration on aviation security](#).

#### *Maritime cargo security*

The air cargo security agreement was preceded in May 2012 by the EU-US mutual recognition agreement on [maritime cargo security](#), whereby the EU and US [recognise](#) their respective 'trusted shippers' programmes – the US Customs-Trade Partnership against Terrorism (C-TPAT) and the EU's Authorised Economic Operators (AEO) regime – and aimed at speeding up customs procedures for cargo scanning.

Customs [cooperation](#) between the EU and US is based on a 1997 agreement and further expanded through a 2004 agreement, which calls, among other things, for the extension to EU ports of the US Container Security Initiative (under which US customs officials, located in foreign ports, help screen maritime cargo containers bound for the US for explosives or weapons of mass destruction). In 2011, a [Joint Statement on Supply Chain Security](#) was issued, whereby the EU and US pledged to increase transatlantic cooperation related to customs security. Tensions in this area have emerged however over US legislation that sets a five-year goal, beyond which all containers bound for the US would be [scanned](#) for nuclear devices, which the EU [finds](#) unrealistic and costly.

### **An assessment of transatlantic cooperation and remaining challenges**

Since 2001, the EU has seen enhancing cooperation with the USA in the JHA area as a key priority, in particular on law enforcement and counter-terrorism. The US has also proactively increased its involvement and supported cooperation with the EU as an actor in its own right in this field. According to reports by the EU Counter-terrorism Coordinator (in [2009](#) and [2011](#)), there has been 'no significant counter-terrorism investigation' in Europe in which US support did not play a crucial role. Moreover, from the US point of view, law enforcement efforts that successfully averted and tracked terrorist plots were the [result](#) of enhanced border security, and advanced passenger information and PNR transfers.



In this context, through mutual learning that has influenced the practice of internal security on both sides of the Atlantic, a process of [policy convergence](#) has been observed by some experts. Some US initiatives and closer transatlantic cooperation seem to have influenced the EU (and also helped shape an [EU interest](#) in the field of counter-terrorism), visible for example in the proposals for an EU-wide agreement on exchanging PNR or the negotiation of such agreements with other third countries; similarly, US officials have recognised the role of the EU in informing some US policies (e.g. in ensuring redress for passengers' complaints about airport screening). Conversely, other experts have [pointed](#) either to the 'Americanisation' of European policy or have [argued](#) that EU-US JHA cooperation has not been a relationship of equals, but mainly a 'one-way street' for providing the US with access to personal data and databases in the EU, without the US sharing its own databases.<sup>11</sup>

In general, important [challenges](#) remain for transatlantic cooperation, all the more complicated by the 2013 revelations of US mass surveillance activities and allegations of data collection in Europe, as well as due to major [differences](#) between the EU and US over strategies to counter the terrorist threat. Europeans have been concerned about American departure from the rule of law in its treatment of terrorist suspects, and pointed to major fundamental rights questions – in particular issues related to data protection and data privacy, posed by the operation of the information-sharing agreements concluded between the EU and the US (both the TFTP/SWIFT and PNR agreements have raised legal problems, including fair procedures, access to justice, fundamental rights, privacy and proportionality), as well as by US practices of extraordinary rendition and secret detention facilities overseas, and by US [detainee](#) policies.

Data privacy still constitutes the main bone of contention in the transatlantic relationship, due to different and seemingly irreconcilable legal systems and traditions in the EU and USA, but also stemming from their differing [geostrategic positions](#). On this issue, some specialists [argue](#) that, despite having criticised the US for privileging security measures over adequate data privacy and data protection standards, the EU finds itself, paradoxically, in the process of adopting the same security-centred approach over privacy rights. For them, the EU would [move closer](#) to the US and would 'shift ... emphasis away from data privacy and toward protective anti-terrorist surveillance programmes'. Conversely, some American observers [deplore](#) the insistence of Europeans on protecting privacy, and underline that the intelligence gathered by the USA, using huge intelligence resources that Europeans could not expect to match, also defends Europeans. Data protection issues notwithstanding (including [US complaints](#) of cyber-cooperation with Europol being severely hindered by data protection concerns), at least as regards the transatlantic [cyber-partnership](#), cooperation seems to be based on solid norms and converging objectives (fighting cybercrime, limiting malicious software and securing critical infrastructure, while promoting international standards for cyberspace).

In all areas, from counter-terrorism to border security and cybersecurity, the EU and the US seem still to be struggling to find the appropriate [balance](#) between strengthening security and facilitating legitimate transatlantic mobility and commerce.

Finally, a further [difficulty](#) stems from the EU institutional setting, with most actions in the field of the judiciary and police pertaining to the national level. In particular, most transatlantic counter-terrorism cooperation is [assessed](#) as still taking place at bilateral

level, between the USA and European national authorities; moreover, US critics [doubt](#) the usefulness of cooperating with EU bodies given these good bilateral ties.

#### Evaluation of EU-US information-sharing agreements

**TFTP/SWIFT:** According to a [report from the EU's Counter-Terrorism Coordinator](#) (November 2015), the EU-US TFTP has generated more than 14 500 intelligence leads since it came into force in 2010. In 2015, 7 514 intelligence leads of relevance were generated, 2 765 of which specifically related to foreign terrorist fighters. Four [evaluations](#) of the agreement have taken place and another was scheduled for late 2015. The reports from [2013](#) and [2014](#) underlined the value of the TFTP data, including data retained over several years, for counter-terrorism investigations both in the US and the EU. The reports give concrete examples of investigations using TFTP data, including the 2013 Boston Marathon bombings, threats to the 2012 London Olympics, and the 2011 attacks in Norway by Anders Breivik. The TFTP agreement is considered an important tool, providing timely and reliable information on activities associated with suspected terrorist acts, although other [experts](#) insist that more information is necessary in order to assess the effectiveness of the TFTP. The joint reviews conclude that Europol and EU Member States are increasingly aware of profiting from TFTP data through the reciprocity clauses of the agreement. A September 2015 [assessment](#) of Europol's implementation of the TFTP also noted the increase in information received since December 2012 and the growing number of requests related to foreign fighters. While the Commission welcomed in 2014 more transparency from US authorities in sharing information, the Treasury Department underlined the need for more feedback from EU and national authorities after the US provides TFTP data.

**EU-US PNR:** A first [joint review](#) of the agreement (Commission and US DHS) was carried out in July 2013 and the next joint review was to take place in July 2015. The first review concluded that the PNR agreement served the purpose of supporting the fight against terrorism and other transnational crimes in various ways. However, some improvements were still needed on the DHS side, including, to 'ensure reciprocity and pro-actively share individual PNRs and analytical information flowing from PNR data with EU Member States and, where appropriate, with Europol and Eurojust'. Another [review](#) performed by the DHS in June 2015 mentions that almost all the recommendations of the 2013 joint review have been implemented, and underlines that between October 2014 and February 2015, the DHS liaison officer submitted 122 names of suspected terrorists to Europol.

**EU-US MLA:** The MLA is being [reviewed](#) after five years; the EU proposed to finalise the joint review by June 2016. Both sides agree that the MLA works well, similarly to the EU-US extradition agreement, but several improvements could be made. On the US side, concerns relate to being overburdened and to the necessity of sharing information more quickly; to tackle this, the US pledged to increase resources and staff in the MLA department. On the EU side, the main concerns related to delays in execution, as well as the necessity to improve electronic means of communication in the MLA context and access to electronic evidence.

#### European Parliament

Since the entry into force of the Lisbon Treaty in 2009, the EP acts on a par with the Council in legislating in the fields of police and criminal cooperation. The Lisbon Treaty also increased the EP's [oversight of Europol](#) (the EP together with the Council decides on regulations setting out Europol's legal framework, while parliamentary scrutiny of Europol's activities should be done by the EP together with national parliaments) and Eurojust. Importantly, the EP has to consent to international agreements concluded by the EU with third countries in this policy area. Parliament's increasing oversight powers became evident when it voted down the TFTP/SWIFT agreement in February 2010, triggering new negotiations to take into account the EP's concerns on data privacy and recommendations.<sup>12</sup> Also in 2010, the EP [postponed](#) its vote on the 2007 EU-US PNR

agreement until the Commission issued its global PNR strategy, after which the EP endorsed the opening of new negotiations with the US. The EP insisted however on a necessary and proportional exchange of data, not using PNR for data mining or profiling, and also expressed concerns about the period for retention of the data.

In light of the revelations of the US large-scale surveillance programmes, the EP adopted a [resolution](#) in March 2014 calling for the suspension of all data transfer agreements with the US (TFTP, PNR), the suspension of the Commission's Safe Harbour Decision, as well as an in-depth assessment of the EU-US MLA and extradition agreements, and requesting the resumption of negotiations on the Umbrella Agreement, which should provide 'effective and enforceable administrative and judicial remedies for all EU citizens in the US without any discrimination' and a high level of [protection](#) of personal data, as a precondition for restoring trust in the transatlantic partnership. The EP also [linked](#) its consent to the Transatlantic Trade and Investment Partnership agreement to ending US mass surveillance activities and to adequate data privacy rights for EU citizens. In October 2015, the EP adopted a [follow-up resolution](#) reiterating its call for the suspension of the TFTP agreement and urging the Commission to assess the legal implications of the Court of Justice ruling of 6 October 2015 in the *Schrems* case vis-à-vis any agreements with third countries allowing for the transfer of personal data, including the TFTP Agreement, all PNR agreements and the EU-US Umbrella Agreement.

## Main references

[U.S.-EU Cooperation against Terrorism](#), Archick K., Congressional Research Service, RS22030, 2 March 2016.

## Endnotes

- <sup>1</sup> Historically, the US maintained important bilateral relations with European states on law enforcement and followed with interest the beginning of cooperation on criminal matters among European states with the [purpose](#) of fighting organised crime, drug trafficking and terrorism – e.g. the 1976 [Trevi Group](#), which included working parties on terrorism and internal security. By the end of the 1980s, criminal law enforcement issues figured regularly on the agenda of meetings between the US, some EU Member States and the Commission, with the US recognising the added value of the progressive 'Europeanisation' of measures in this field. Counter-terrorism issues have been part of the transatlantic dialogue since 1986. See 'External relations of the EU with the US in counter-terrorism' in *The Evolving EU Counter-Terrorism Framework*, O'Neill M., 2012, pp. 164-188.
- <sup>2</sup> The EU and USA also cooperate within [multilateral frameworks](#), such as the Global Counterterrorism Forum (GCTF), where they promote international cooperation on counter-terrorism and countering violent extremism, as well as offer assistance to third countries for capacity building in the justice and rule of law areas.
- <sup>3</sup> See also ['Foreign fighters' - Member States' responses and EU action in an international context](#), Bakowski P., Puccio L., EPRS Briefing, March 2016.
- <sup>4</sup> Bulgaria, Croatia, Cyprus, Poland and Romania are the five EU Member States not yet included in the US VWP.
- <sup>5</sup> 'La coopération transatlantique en matière de cybersécurité', Joubert V., in *Vers un partenariat transatlantique de l'Union européenne*, Auvret-Finck, J. (Ed.), Larcier, 2015, pp. 271-288.
- <sup>6</sup> [U.S.-EU Cooperation against Terrorism](#), Archick K., Congressional Research Service, RS22030, 1 December 2014.
- <sup>7</sup> [Handbook on the practical application of the EU-U.S. Mutual Legal Assistance and Extradition Agreements](#), Council of the EU, 8024/11, March 2011.
- <sup>8</sup> There are still [calls](#) for the establishment of a European TFTP programme, which the Commission had [assessed](#) in 2013 as very costly and not bringing significant added value to the current situation.
- <sup>9</sup> The PNR agreement is restricted to those transnational crimes punishable by a sentence of imprisonment of three years or more – as demanded by the European Parliament.
- <sup>10</sup> Court of Justice ruling of 6 October 2015 in the *Schrems* case ([C-362/14](#)). Essentially, the Court ruled that: i) the generalised transfer of data under the Safe Harbour scheme without determining the limitation of access of US public authorities to the data was 'compromising the essence of the fundamental right to respect for private life'; and ii) the lack of access to legal remedies for individuals concerning their personal data was in breach of their fundamental right to effective judicial protection. See also [The CJEU's Schrems ruling on the Safe Harbour Decision](#), Monteleone S., Puccio L., EPRS, October 2015.

<sup>11</sup> [Experts](#) also point to US demands for [access](#) to criminal records across the EU, which they deem controversial.

<sup>12</sup> 'Parliamentary oversight of counter-terrorism policies', Oikarinen J., in *Counter-terrorism: International law and practice*, Salinas de Frías A. M., Samuel K., White N.D. (Eds.), Oxford, 2012, pp. 936-964.

## Disclaimer and Copyright

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2016.

Photo credits: © jamdesign / Fotolia.

[eprs@ep.europa.eu](mailto:eprs@ep.europa.eu)

<http://www.eprs.ep.parl.union.eu> (intranet)

<http://www.europarl.europa.eu/thinktank> (internet)

<http://epthinktank.eu> (blog)

