Briefing
June 2015

US policy to bring terrorists to justice

SUMMARY

US counter-terrorism strategy continues to be at the centre of public attention, with the recent drone strike, killing Yemeni al Quaeda leader Nasir al-Wuhayshi on 16 June 2015. The US government relies on a wide range of tools, inter alia intelligence, law enforcement and foreign policy.

US measures to bring terrorists to justice are still being debated and slowly redefined, primarily through court rulings assessing their compatibility with US constitutional law. The United States' criminal law has been broadened in scope, with wide extraterritorial application allowing prosecution of terrorists of other nationalities committing crimes outside the US. Certain measures taken in parallel to the domestic criminal procedure, such as the institution of ad hoc military commissions and the retention of prisoners in Guantanamo, have been challenged in the courts.

The counter-terrorism strategy relies on surveillance machinery involving various actors at the federal and state level, whose task is to identify suspects and gather evidence. The use of technology has created new opportunities for security controls but has also shown how difficult it is to strike a balance between the protection of rights, such as the right to privacy, and these new surveillance methods. The debates on the NSA surveillance programme and the court cases on the No Fly List are but examples of a broader debate on the human rights limits of some security measures taken to fight terrorism.

The US deems its collaboration with international actors and the EU in this domain as essential, not least because the functioning of its surveillance apparatus depends in part on information gathered abroad. However, concerns persist over the eventual implications for constitutional rights and freedoms that the US model entails, and these have become one of the major sources of opposition to the Transatlantic Trade Investment Partnership with the US. A new act has been introduced in the US Senate proposing the extension of redress rights under the Privacy Act to major US allies.

In this briefing:

EPRS | European Parliamentary Research Service
Author: Laura Puccio
Members' Research Service
PE 564.384

Background and issue

The 9/11 terrorist attacks shook the US to the core and brought calls for a major reorganisation of its counter-terrorism strategy. Consequently, the post-9/11 era has been characterised by the definition of new intelligence methods and programmes, as well as by the adoption of new laws to prosecute terrorist activities and terrorism-related crimes. Many of the initial actions taken were based on the Congressional Authorization for Use of Military Force, a resolution granting the US President authority to 'use all necessary and appropriate force' against the masterminds of the attacks. Some actions were taken via presidential orders but many others were codified in the Patriot Act and its subsequent revisions. The Patriot Act more particularly introduced new criminal law provisions, authorised new surveillance programmes and spurred the initiation of actions against international money laundering and the financing of terrorism.

The more recent events associated with the rise of Islamic State of Iraq and the Levant (ISIL), also known as Da'esh, and the debates on how to deal with the issue of foreign fighters (i.e. individuals who join conflicts abroad, in this context those who join jihadist movements for ideological or religious reasons) have made it worthwhile examining the policies the United States employs to bring terrorist to justice (both legal provisions to prosecute terrorists and the surveillance apparatus used for gathering information on suspects) and review some of the main public and legal debates they have raised.

Indeed some of the actions taken in the name of security (such as the military commissions or the No Fly List) have been, and still are, challenged via courts and public debate on the grounds of their legality with respect to US constitutional and fundamental rights. Achieving a balance between security and fundamental constitutional protection is difficult and still far from being a fact, as demonstrated by the recent revelation that the CIA still applies torture in the form of 'enhanced investigation techniques', techniques that were allowed in 2002 under the Bush administration but later prohibited by an executive order issued by Obama in 2009. Progressive limits imposed on governmental action in the field with a view to curtailing abuse have also partly stemmed from long and difficult court proceedings.[1]

US foreign policy contributes substantially to the US counter-terrorism strategy for at least two reasons: first, to enable it to assist in the gathering of or access to information collected by foreign allies; and second, to ensure that partners prosecute local terrorists directly, thereby avoiding legal proceedings taking place in the US. The US has, inter alia, influenced new criminal legislation abroad (e.g. in Bangladesh), and its international agreements, including those with the EU, have been fully integrated into the extensive governmental surveillance machinery that has slowly been put in place to cope with terrorist threats. Transatlantic cooperation to combat terrorism and global threats from violent extremism was high among Vice-President Joe Biden's priorities during his meeting with European Council President, Donald Tusk in Brussels on 6 February 2015. Terrorist and extremist threats have also become a key priority for European governments following the recent events in Paris and Copenhagen, and most recently targeting European holiday-makers in Tunisia. In their cooperation in the field, the EU and the US are still actively searching for ways to provide citizens on both sides of the Atlantic with the highest possible protection of their fundamental rights and to ensure them proper rights of redress.

Punitive measures

Prosecution of terrorism and terrorism-related activities

Prosecution of 'material support to terrorist organisations' is done through a series of laws enacted in 1994 and amended after 2001 by the Patriot Act. These measures concern direct participation in terrorist acts, as well as all kinds of material support (e.g. money or weapons) and intangible aid in the form of training and expert advice or assistance. The most recent indictment from 5 February 2015 was brought against six Bosnians for supplying money and equipment to terrorist groups. In another case involving an NGO set up with the aim of facilitating UN negotiations with terrorist groups from Tamil and Kurdistan, the US Supreme Court ruled that any action falling under the Patriot Act, such as a financial transfer or assistance to a terrorist organisation, is punishable regardless of the existence of criminal intent.[2] Some measures may also be applied to non-US citizens through extraterritorial jurisdiction. The Manhattan Federal Court confirmed in a recent case that extraterritorial jurisdiction is certainly exercised when explicitly mentioned in the relevant statute.[3] US provisions on extraterritoriality have a broad scope of application; beyond traditional extraterritorial jurisdiction claims,[4] extraterritoriality has also been exercised in accordance with the 'protective principle' which gives jurisdiction to a country over actions undertaken by foreigners outside its territory when these actions are against its interests.[5]

Table 1: US criminal law provisions applicable to foreign fighters

Statute provisions	Crimes	Extraterritorial jurisdiction clause
18 USC§956	Conspiracy to kill, kidnap, damage property in a foreign country	No
18USC§2332a	Use of weapons of mass destruction	Yes, limited to US nationals
18USC§2332b	Acts of terrorism transcending national boundaries	Yes
18USC§2332f	Bombing of public government facilities	Yes
18USC§2339	Harbouring or concealing terrorists	No
18USC§2339a	Providing material support to terrorists (any tangible or intangible support including supply of goods as well as financial, assistance and training supports)	No
18USC§2339b	Providing support to foreign terrorist organisations	Yes
18USC§2339c	Prohibitions against the financing of terrorists	Yes
18USC§2339d	Receiving military training from a foreign terrorist organisation	Yes

Source: Author, from 18 US Code Chapter 113B.

Non-traditional law enforcement measures and rights violations

Notwithstanding the existence of the US criminal law provisions mentioned in table 1, many cases related to terrorist activities have actually been prosecuted under military authority and law, especially, but not exclusively, when the combatant has been apprehended in the conflict area and is not a US citizen. The Bush administration issued a series of measures to avoid applying the ordinary court proceedings to unlawful combatants arrested during the conflict in Afghanistan. The result was the creation of a parallel justice system whose boundaries and constitutional guarantees have been constantly redefined by the courts ever since and are still in need of clarification.

In 2001, President George W Bush decided to use the Guantanamo Bay facility for the detention of prisoners assigned the status of 'enemy combatants'. This term was first

used and defined in the *Ex parte Quirin* case,[6] in which the Supreme Court distinguished between 'enemy belligerents' within the meaning of the Hague Convention (1907) and the law of war, and 'unlawful combatants', who, without wearing uniforms, have waged war outside the laws of war and who have not been deemed to be entitled to the status of 'prisoners of war'. In the *Ex parte Quirin* case it was decided that 'unlawful combatants' would be prosecuted by military tribunals. Using this case as a legal basis, Bush enacted the original Military Order (MO) authorising military trials of the Guantanamo detainees, and specifying that they would not be granted any recourse under the US court system. The Bush administration did this with the aim of avoiding claims invoking federal courts' jurisdiction or requesting prisoner-of-war status under the Geneva Convention. These measures were challenged on two grounds: (1) 'enemy combatants' who were detained without proper trial asserted their rights to due process in court, and (2), those subject to a military tribunal challenged its legality under US military law.

The first challenge with regard to due process was done by the detainees claiming *habeas corpus* rights. *Habeas corpus* is a recourse in law where the legality of a prisoner's detention is challenged and whereby the prisoner may demand a trial to prove his/her innocence. Initially, the claims were unsuccessful in lower courts. The latter considered Guantanamo to be out of the US courts' jurisdiction and therefore denied *habeas corpus* writs to the detainees. However, in its judgment on *Rasul* v. *Bush* (2004), the Supreme Court held that prisoners had a right to *habeas corpus* writs on two grounds: firstly, *habeas corpus* had to be attributed on the basis of the nationality of the authority detaining the prisoner (the custodian), and not the nationality of the prisoners; and secondly, Guantanamo was under exclusive US control.[7] In response to the Supreme Court, the US Congress enacted the Detainee Treatment Act (2005), revoking judicial jurisdiction over *habeas* claims by persons detained as enemy combatants. The *habeas corpus* right was reasserted in 2008 by the *Boumediene* case, in which the Supreme Court[8] declared the Detainee Treatment Act unconstitutional. While the *habeas corpus* right is now ensured, its scope is still uncertain. For example, it is not yet clear whether detainees have the right to challenge in federal courts and obtain remedy for mistreatment during detention. Recourse to local and federal courts has also been introduced to ensure compliance with other constitutional rights such as the right to counsel.[9]

The second challenge regarding the legality of the military commissions that had been established was submitted to the Supreme Court in the *Hamdan* v. *Rumsfeld* case (2006).[10] The Supreme Court found that military tribunals established under the Military Order of 2001 were unlawful, because they did not abide by the Uniform Code for Military Justice (UCMJ), which is the foundation of military law in the US, and the common law of war. The US Congress then adopted the Military Commissions Act (MCA 2006), which still departed in significant ways from the rules enshrined in the UCMJ, but narrowed the scope of the military commissions' jurisdiction to trials of unlawful enemy combatants. After President Barack Obama took office, an amended Military Commissions Act (MCA 2009) was passed. The new act no longer refers to 'lawful' and 'unlawful enemy combatants', but to 'privileged' and 'unprivileged belligerents'. The change in definition does not seem to bring much novelty, and the definition of 'unprivileged enemy belligerent' actually seems potentially wider in scope than its predecessor (see box below). That said, the MCA 2009 did bring some significant changes.[11] In particular, it gave military commissions the authority to establish before

the inception of each case whether they have jurisdiction or not, i.e. they decide on the status of the detainees, and the prosecution has the burden of proving that the military commission has jurisdiction over the detainees.

Table 2: Comparing definitions of combatants in the MCA (2006) and the MCA (2009)

Military Commissions Act (2006)	Military Commissions Act (2009)
''(1) UNLAWFUL ENEMY COMBATANT.—(A) The term 'unlawful enemy combatant' means—(i) a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States or its co-belligerents who is not a lawful enemy combatant (including a person who is part of the Taliban, al Qaeda, or associated forces);or (ii) a person who, before, on, or after the date of the enactment of the Military Commissions Act of 2006, has been determined to be an unlawful enemy combatant by a Combatant Status Review Tribunal or another competent tribunal established under the authority of the President or the Secretary of Defense. ''(2) LAWFUL ENEMY COMBATANT.—The term 'lawful enemy combatant' means a person who is—(A) a member of the regular forces of a State party engaged in hostilities against the United States; (B) a member of a militia, volunteer corps, or organized resistance movement belonging to a State party engaged in such hostilities, which are under responsible command, wear a fixed distinctive sign recognizable at a distance, carry their arms openly, and abide by the law of war; or (C) a member of a regular armed force who professes allegiance to a government engaged in such hostilities, but not recognized by the United States.	**(6) Privileged belligerent.—** The term ''privileged belligerent'' means an individual belonging to one of the eight categories enumerated in Article 4 of the Geneva Convention Relative to the Treatment of Prisoners of War. (7) **Unprivileged enemy belligerent.—** The term ''unprivileged enemy belligerent'' means an individual (other than a privileged belligerent) who— (A) has engaged in hostilities against the United States or its coalition partners; (B) has purposefully and materially supported hostilities against the United States or its coalition partners; or (C) was a part of al Qaeda at the time of the alleged offense under this chapter.

Source: Author, 2015.

Another major change brought in by the MCA 2009 is the express prohibition of the use of statements obtained under coercion and torture. While the MCA 2006 had made a distinction between statements obtained under coercion and torture, that distinction was abolished. This change was meant to completely dissuade law enforcement authorities from using 'enhanced' investigation techniques. These techniques had been authorised under the Bush administration through a series of legal opinions often referred to as 'torture memos', asserting the legality of some investigative methods that used torture-like methods in the framework of the 'war against terror'. When assuming office, President Obama had prohibited these methods and repealed all legal opinions and executive orders that had sanctioned their use. A review conducted by the Senate on CIA investigation methods revealed in December 2014 that the eradication of such methods is still far from being fully implemented. On 16 June 2015, the Senate voted in favour of a bill banning torture during prisoners' interrogations by the military and by all other governmental institutions.

Surveillance and intelligence

The United States' domestic and international activities in the area of counter-terrorism have been primarily focused on increasing the monitoring and prosecution of terrorist activities in order to identify suspects and gather sufficient evidence to bring them to court. These activities are carried out by a large number of institutions, including intelligence agencies, the National Counter-terrorism Centre, the Department of Homeland Security, the Justice Department, Treasury Department, the FBI, the military, embassies, and others. The 'whole-of-government' approach adopted in the 2010 US National Security Strategy aims to limit competition and increase information-sharing among government agencies and departments, as a way to ensure enhanced monitoring and investigative capacity and boost law enforcement as a whole. In

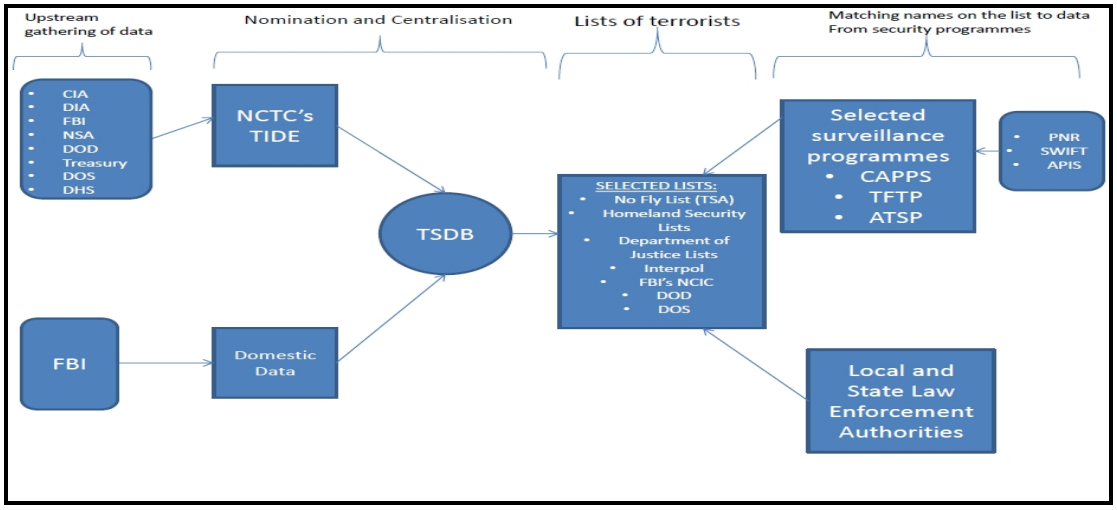
particular, information among federal, state and local governments is shared through the Joint Counter-terrorism Assessment Team.

Surveillance and coordination of information

An entire apparatus has been created to disseminate information on suspected terrorists and to process new information for monitoring. The 'whole-of-government' effort to streamline and disseminate information among federal authorities and departments as well as state and local governments is illustrated in figure 1 below.

The National Counter-terrorism Centre (NCTC) maintains the Terrorist Identities and Datamart Environment (TIDE) – the US government's central repository of information on international terrorist identities. Several institutions contribute to TIDE, including: the CIA, the Defense Intelligence Agency (DIA), the Department of Defense (DOD), the Department of State (DOS), the Treasury Department, the Department for Homeland Security (DHS), the FBI, and the National Security Administration (NSA). One of the programmes that contribute to this upstream information-gathering, and to TIDE, is the controversial NSA-run Domestic Surveillance Program, which is used for obtaining telephony and internet metadata, i.e. information about the context rather than the content of internet and communications connections. Such information includes calling records, localisation of persons via their mobile phones, and social network connections. Once gathered, this information makes it possible to 'map' the profiles of suspected individuals and groups (through data mining and social network analysis).[12]

Figure 1: Streamlining information



Source: Author, 2015.

In addition to programmes used for identifying suspects, such as the NSA Domestic Surveillance Program described above, other databases with the names of known or suspected terrorists are also being kept. These names are consolidated by the FBI's Terrorist Screening Centre in the Terrorist Screening Database (TSDB), also known as the 'Watchlist'. The information contained in the TSDB feeds into the databases maintained by various other agencies and departments such as the Departments of Homeland Security, State, Justice and Defense. Within the TSDB, the data supplied by TIDE are complemented by domestic data (i.e. on terrorists operating within the US but not connected to international terrorism).

A subset of nominees from the TSDB is then placed on a number of different security lists, one of which is the No Fly List, containing the names of suspects not allowed on flights in and out of the US. The Transportation Security Administration (TSA) is in

charge of matching the names on this list with information provided under the Secure Flight Program.[13] This information includes name, date of birth, gender, known traveller number and redress number, allowing the TSA to ground suspected terrorists before they board a plane.

There are also other subset lists: each of the above-mentioned departments has at least one such list of suspects they check. Information collected through the various surveillance programmes is matched against the names on these lists. For example, using the Automated Targeted System for Passengers (ATSP), the Customs and Border Protection Agency verifies and compares PNR and Advanced Passenger Information System (APIS) data to the information contained in various law enforcement databases, inter alia from immigration system databases and US Treasury Department databases. Another such example is the Terrorist Finance Tracking Program (TFTP), initiated by the US Treasury Department in order to identify, track, and pursue terrorists and their networks. This programme has access to the information contained in the worldwide financial transactions database maintained by SWIFT, the Belgium-based Society for Worldwide Interbank Financial Telecommunication. It uses this information to track the financial transactions of individuals on the suspected terrorist lists, to track the networks that terrorists take part in and to identify further suspects, as well as to locate operatives and financial networks the terrorists use. This makes it a source of upstream evidence that can be used to justify nomination to the TSDB.

Selected issues regarding the surveillance programmes

The surveillance machinery created to gather intelligence and evidence has been seriously debated upon by civil society and academia because of the potential conflicts vis-à-vis US constitutional rights. For example, the NSA's Domestic Surveillance Program came under attack after one of its former contractors, Edward Snowden, made public revelations in 2013 about its practices. This raised a debate in the US on the programme's legal implications (both for freedom of expression under the First Amendment and for data protection under the Fourth Amendment).[14] Doubts were cast on the potential of the techniques employed, such as data mining and social network analysis, to identify real criminal intent. Indeed, data mining could raise unjustified suspicions of criminal intent in situations where freedom of expression is involved. Moreover, the NSA programme did not need a warrant to start surveillance. The Fourth Amendment would normally require a warrant to be obtained before undertaking surveillance or information-gathering. However, the NSA programme was considered to be in line with US data protection legislation because the Fourth Amendment was currently only applicable to content information and not to metadata, which was the focus of the NSA surveillance programme. Indeed the Supreme Court case *Katz* v. *United States* applied the Fourth Amendment to the content of telephonic conversations, while the Supreme Court case *Smith* v. *Maryland* denied applicability of the Fourth Amendment to the telephone numbers dialled. These court cases are at the basis of the distinction between '**content**' (for example the content of a letter) and **'incidental information' or metadata** (for example the address on an envelope and the name of the addressee). In the *Klayman* v. *Obama* case, decided in December 2013, a federal court ruled that the collection of metadata by the NSA was still in violation of the US constitution. The court stated that the *Smith* v. *Maryland* judgment only allows **short-term forward-looking capture**, while the NSA is using the metadata for **long-term historical retrospective analysis.** The *Klayman* v. *Obama* case has not been overruled but has some negative history as courts in subsequent cases have decided not to follow

the same path of reasoning.[15] Another case in front of the United States Court of Appeals concluded that in running its Domestic Surveillance Programme, the NSA exceeded the scope of what Congress had authorised under section 215 of the Patriot Act and that the NSA therefore lacked congressional authorisation to run the Domestic Surveillance Program.

The debate surrounding the NSA has prompted the submission of a legislative initiative, proposing to make the Fourth Amendment also applicable to telephony and internet metadata under the Electronic Communication Privacy Act. Moreover, the US legislature has been debating how to amend procedures for physical and electronic surveillance under the Foreign Intelligence Surveillance Act (FISA), in order to enhance data protection. The FISA was amended under the Bush administration to give the green light to counter-terrorism surveillance programmes. Debate on the USA Freedom Act, passed by the House of Representatives in 2014 and allowing a compromise between security and privacy, had to be postponed to 2015, after the Senate voted a motion of closure that postponed discussions on the matter until later in 2015.

US legislation regulating surveillance

Foreign Intelligence Surveillance Act: regulates physical and electronic surveillance and the collection of 'foreign intelligence information' (information on 'agents of foreign powers', including US citizens).

Electronic Communication Privacy Act: regulates surveillance of transmissions of electronic data by computer, access to stored electronic communications, metadata accessibility.

Freedom of Information Act: regulates the disclosure of information controlled by the US government.

Privacy Act: establishes a code of fair information practice that governs the collection, maintenance, use and dissemination of personally identifiable information maintained in records of federal agencies.

The nomination of suspects to the TSDB and to the subset lists of terrorists also raises several legal issues, in particular with respect to due process and to whether the suspicion leading to the inclusion of that name has been sufficiently grounded. Several cases have been brought before the courts because of the implications related to a person's nomination to the No Fly List, in particular the severe restriction of movement implied by the ban on taking flights to or from the US.[16] In 2014, a federal court stated that the No Fly List nomination procedure violated due process rights, and declared unconstitutional the existing procedure to obtain redress from nomination to the No Fly List, requiring the government to amend it. The court held, among other things, that the defendant must provide the plaintiffs with notice regarding their status on the No Fly List and, without creating an undue risk to national security, a statement of the reasons for including each plaintiff on the No Fly List in order to permit each plaintiff to submit evidence challenging their placement on the list. [17]

It seems that the ongoing debates in the United States about the possibility of withdrawing the US citizenship of individuals fighting alongside a terrorist organisation abroad are linked to the recent legal issues connected to the implementation of the No Fly List, used until now as the main instrument for refusing terrorist suspects the possibility to return to the US. Denationalisation is not feasible under current US law, which envisages a loss of US citizenship only in very exceptional circumstances. A legislative initiative has been submitted to Congress recently, proposing to include terrorism as a ground for loss of nationality. Apart from the United States' own constitutional limits, there do not seem to be any international limits to the use of denationalisation. Indeed, the US is not a party to the UN Convention on the Reduction of Statelessness, which prohibits the removal of citizenship that would result in a situation of statelessness.

The international dimension of US counter-terrorism policy

Given the global nature of terrorism, the US has been extremely active in trying to secure the collaboration of other countries for gathering evidence and apprehending foreign fighters.

In this respect, US international efforts have been directed towards arming partners with penal rules to prosecute terrorists, including foreign fighters, locally.[18] Pressure has been put to that effect on less collaborative partners through the adoption of multilateral instruments such as UN Security Council Resolution 2178, but also through the so-called 'End Financing ISIL' bill. This unilateral bill suspends any military assistance in the form of military sales authorisation and military financing to countries which have not taken action against persons providing material or financial support to ISIL/Da'esh while located in the said countries.

Furthermore, softer collaboration programmes have been introduced for potentially more fragile countries as a way to avoid their becoming a safe haven for terrorist activists. In particular, the focus has been on countries whose fragile banking systems make them susceptible to becoming money laundering centres. This has involved reinforcing customs cooperation via training, as well as providing legal advice and help to revise and strengthen their rules against terrorism. For example, the US provided Bangladesh with technical assistance to revise and amend its Antiterrorism Act. Adopted in 2013, the new act introduced extensive provisions for the criminalisation of terrorist financing and banned support for individuals (rather than simply organisations) engaging in terrorist activity. It also introduced the possibility to rapidly freeze the funds and assets of those engaged in, or supporting, terrorism. Moreover, the US has initiated several counter-terrorism capacity-building programmes with African countries. Following a meeting with the European Union, the Department of Justice announced in November 2014 that it would send prosecutors jointly with FBI agents to advise and to assist officials investigating and prosecuting foreign fighters in Balkan, Middle East and Northern African countries.

EU-US relations and counter-terrorism

The US has always recognised the EU as a key partner in law enforcement against terrorism.

In the aftermath of 9/11, EU-US cooperation in data-sharing and border security activities was sealed with several agreements.[19] These information-sharing agreements complement existing US surveillance programmes. For example, data from PNR agreements, including from the Agreement concluded in 2011 between the EU and the US Agreement on the use and transfer of passenger name records (PNR) to the US Department of Homeland Security, are processed by the US customs authority (CBP) and Transportation Security Administration as part of their respective passenger and cargo surveillance programmes. Similarly, the so-called Swift Agreement, allowing US and EU authorities to access financial data held by the Belgian consortium of banks known as SWIFT, is an integral part of the US Treasury Department's Terrorist Finance Tracking Program. The US also has an agreement with Europol and Eurojust for cooperation in investigations and exchange of information on suspected terrorists; moreover, some EU Member States collaborate with the US within the Interpol Foreign Terrorist Fighter Program. The US has concluded two agreements with the EU which have been in force since 2010, on mutual legal assistance and on extradition. It is

important to point out that Article 13 of the Agreement on Extradition prohibits the death penalty from being applied or carried out.

While the above-mentioned agreements have earned credit for enhancing security and fighting terrorism, tensions remain with respect to their implications with regard to data protection. In response to the NSA scandal, the European Parliament voted in March 2014 a resolution on the basis of the Moraes Report, containing a number of recommendations for future EU-US relations. The fate of the EU-US PNR agreement may well rest partly on the opinion of the Court of Justice of the EU, requested by the European Parliament, on the legality of the EU-Canada PNR with respect to the Charter of Fundamental Rights and to data protection. Considering the likely involvement of some internet companies (such as Google, Yahoo, and Facebook) in the NSA surveillance programme, the European Parliament voted for amendments to the proposed reform of EU data protection rules, requiring US-based internet firms to request authorisation before complying with US warrants for the data of EU citizens. This reform proposal is still awaiting approval from the Council of the European Union.

Most of the EU-US agreements have clauses or supplementary agreements to ensure that they are in line with EU requirements on data privacy. Currently, only US citizens and permanent residents in the US have access to remedies under the Privacy Act.

The US mass surveillance programme scandal, and the issue of limited rights of redress, have been linked in some Member States to the debate on the Transatlantic Trade and Investment Partnership (TTIP), making data protection a key outstanding issue and one of the main sources of opposition to TTIP. The draft recommendations on the TTIP negotiations, adopted by the Committee on International Trade (INTA) of the European Parliament on 28 May 2015, went as far as linking Parliament's consent to TTIP to the dismantling of US mass surveillance programmes and the introduction of a proper redress mechanism for EU citizens.

In this context, the US urged the EU to complete the implementation of the EU PNR system and promised in exchange to issue a legislative proposal enhancing EU citizens' redress rights to protect their data privacy. In line with that promise, the Judicial Redress Act of 2015 was introduced in March in the House of Representative and on 17 June in the Senate; the bill would extend core benefits of the Privacy Act to citizens of major US allies for information shared for law enforcement purposes, and thereby give them redress rights under the act.

Table 3: EU citizens' access to redress under US data protection legislation

US legislation	EU citizen's access to administrative or judicial redress
Foreign Intelligence Surveillance Act (FISA)	Yes
Electronic Communication Privacy Act (ECPA)	Yes
Freedom of Information Act (FOIA)	Yes
Privacy Act	Only to permanent residents in the US

Source: Author, 2015.

In order to find more common ground with regard to the protection of data privacy and to engage in more integrated collaboration, the EU and the US have started negotiating an umbrella agreement on Data Privacy and Protection (DPPA). The DPPA will not empower institutions to exchange data; the latter will remain part of other agreements (such as on PNR and SWIFT). However, the DDPA will focus on ensuring that treatment

and exchange of data under all these agreements is done while maintaining a higher level of data privacy protection, and granting equal rights of access to remedies on both sides of the Atlantic (Article 2(1) in the draft Umbrella Agreement).

A further difficulty in US-EU cooperation stems from the current EU institutional setting; notwithstanding the various competences of the EU on terrorism,[20] the main competence remains in the hands of the Member States. Action in the field of judicial and police affairs is done via cooperation among EU national authorities. Cooperation in intelligence matters is not always effective and the US has often preferred to cooperate directly with national entities.[21]

Main references

K. Archick, US-EU Cooperation against Terrorism, CRS Report, 1 December 2014.

K. Katzman, C. M. Blanchard, C. E. Humud, R. Margesson, M. C. Weed (Jan. 8, 2015), The "Islamic State" Crisis and the US Policy, CRS Report, 11 February 2015.

J. K. Elsea and M. J. Garcia, Judicial Activity Concerning Enemy Combatant Detainees: Major Court Rulings, CRS, 9 September 2014.

Steven Morrison, The System of Domestic Counter-terrorism Law Enforcement, *Stanford Law and Policy Review* vol. 25, 2014

J. K. Elsea, The Military Commission Act of 2009 (MCA 2009): Overview and Legal Issues, 4 August 2014, CRS.

L. K. Donohue (2014), Bulk Metadata Collection: Statutory and Constitutional Considerations, *Harvard Journal of Law and Public Policy* vol. 37 n.3, 2014.

E. Fahey, Law and governance as checks and balances in transatlantic security: rights, redress and remedies in EU-US passenger name records and the terrorist finance tracking program, *Yearbook of European Law* vol.32, 2013.

Endnotes

[1] For more details, see: J. K. Elsea and M. J. Garcia, Judicial Activity Concerning Enemy Combatant Detainees: Major Court Rulings, 9 September 2014, CRS Report.

[2] *Holder* v. *Humanitarian Law Project*, 130 S. Ct. 2705 (2010).

[3] *United States* v. *Mohammed Ibrahim Ahmed* (March 22. 2012), F.Supp.2nd, 2012 WL 983545.

[4] Traditional extraterritorial jurisdiction is based on three main jurisdictions: the nationality jurisdiction, when the criminal committing the crime abroad is a national of the state conducting the prosecution; the passive personality principle, whenever the victim of the crime is of the nationality of the state prosecuting the criminal, and lastly, the more controversial universal jurisdiction, where jurisdiction is based on the nature of the crime considered as a serious international crime (crime against humanity, piracy, slave trade or forced labour).

[5] See the case: *United States* v. *Yousef*, 327 F.3d 56, 90-1 (2d Cir. 2003).

[6] *Ex parte Quirin*, 317 U.S. 1, 37-38 (1942).

[7] The judgment was not unanimous, as in most cases involving terrorism issues. There was one dissenting opinion, which upheld the position of the lower courts, and one concurring opinion, which agreed on the jurisdiction over Guantanamo but refused to admit that jurisdiction in the case of *habeas corpus* writs is dependent on the nationality of the authority detaining the prisoner and therefore denied a general jurisdiction over cases of detention by US forces abroad, claiming that jurisdiction over *habeas corpus* writs depends on whether the US has sovereign jurisdiction over the territory where the detainees are. See: *Rasul* v. *Bush*, 542 U.S. 466 (2004).

[8] *Boumediene* v. *Bush*, 553 U.S. 723 (2008).

[9] *In re: Guantanamo Bay Detainee Continued Access to Counsel*, 892 F. Supp.2d 8 (D.D.C. Sep 06, 2012) (NO. CIV.A. 04-1254 RCL, CIV.A. 05-1638 CKK, CIV.A. 05-2185 RCL, CIV.A. 05-2186 ESH, CIV.A. 05-2380 CKK, MISC. 12-398 RCL).

[10] *Hamdan* v. *Rumsfeld*, 548 U.S. 557 (2006).

[11] For a more detailed analysis on all of the changes introduced by the Military Commissions Act 2009, please refer to: J. K. Elsea, The Military Commission Act of 2009 (MCA 2009): Overview and Legal Issues, 4 August 2014, CRS.

[12] Steven Morrison (2014), The System of Domestic Counter-terrorism Law Enforcement, *Stanford Law and Policy Review*, vol. 25.

[13] The Secure Flight Program replaced the Computer Assisted Passenger Pre-screening System (CAPPS/CAPPS II), after the latter received a failing grade in the protection of privacy from the congressional investigatory office (GAO). CAPPS/CAPPS II gathered information from US travel agencies and matched it against names on the Watchlist in order to stop suspected terrorists from buying airplane tickets.

[14] See, inter alia: Steven Morrison (2014), The System of Domestic Counter-terrorism Law Enforcement, *Stanford Law and Policy Review*, vol. 25; L. K. Donohue (2014), Bulk Metadata Collection: Statutory and Constitutional Considerations, *Harvard Journal of Law and Public Policy,* vol. 37 n.3; J. Joo (2014), The Legality of the National Security Agency's Bulk Data Surveillance Programs, *Harvard Journal of Law and Public Policy,* vol. 37 n.3.

[15] See: *In re Application of F.B.I.*, 2014 WL 5463097 (Foreign Intel.Surv.Ct. Mar 20, 2014) (NO. BR 14-01); *In re Application of F.B.I.,* 2014 WL 5463290 (Foreign Intel.Surv.Ct. Jun 19, 2014) (NO. BR 14-96); *United States* v. *Hassanshahi*, 2014 WL 6735479 (D.D.C. Dec 01, 2014) (NO. CR 13-0274 (RC)); *Competitive Enterprise Institute* v. *National Security Agency*, 2015 WL 151465 (D.D.C. Jan 13, 2015) (NO. CV 14-975 (JEB)); *U.S.* v. *Post*, 997 F.Supp.2d 602 (S.D.Tex. Jan 30, 2014) (NO. 3:13-CR-20); *Robinson* v. *Obama*, 2014 WL 1389020 (D.D.C. Apr 04, 2014) (NO. CV 14-568 UNA); *Smith* v. *Obama*, 24 F.Supp.3d 1005 (D.Idaho Jun 03, 2014) (NO. 2:13-CV-257-BLW); *In re Yahoo Mail Litigation*, 7 F.Supp.3d 1016 (N.D.Cal. Aug 12, 2014) (NO. 5:13-CV-04980)

[16] For an overview, refer to: J. P. Cole, The No Fly List: Procedural Due Process and Hurdles to Litigation, September 18 2014, CRS. See also, as examples: *Latif* v. *Holder*, 28 F.Supp.3d 1134 (D.Or. Jun 24, 2014); *Ibrahim* v. *Department of Homeland Security*, 2014 WL 6609111 (N.D.Cal. Jan 14, 2014); also see: *Mokdad* v. *Holder*, 2013 WL 8840322 (E.D.Mich. Dec 05, 2013); *Fikre* v. *F.B.I.*, 23 F.Supp.3d 1268 (D.Or. May 29, 2014); *Tarhuni* v. *Holder*, 8 F.Supp.3d 1253, 1271, 2014 WL 1269655 (D.Or. Mar. 26, 2014).

[17] *Latif* v. *Holder*, 28 F.Supp.3d 1134 (D.Or. Jun 24, 2014).

[18] For example: the US involvement in the recent amendments of Bangladesh's counter-terrorism legislation.

[19] On a recent overview of US-EU relations: K. Archick, 'US-EU Cooperation Against Terrorism', *CRS Report* (Dec. 1, 2014).

[20] See: CFSP actions under Article 43 of the TEU and restrictions and sanctions on individuals under Article 215 of the TFEU. Provisions in Part III Title V of the TFEU dealing with the area of freedom, security and justice, including cooperation among various JHA authorities and the possibility for minimum rules and approximation under Article 83 of the TFEU and under Article 82 (judicial cooperation in criminal matters) of the TFEU.

[21] See: the Interpol Foreign Terrorist Fighters programme or the UK's collaboration with the NSA Surveillance Program.

Disclaimer and Copyright

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)