[redacted]

COUNCIL OF
THE EUROPEAN UNION

Brussels, 10 November 2009

15671/09

RESTREINT UE

JAI 813
USA 99
RELEX 1043
DATAPROTECT 71
ECOFIN 719

NOTE	
from :	Presidency
to :	Delegations
prev.doc.:	15397/09 JAI 782 USA 95 RELEX 1009 DATAPROTECT 69 ECOFIN 699
Subject :	Draft Council Decision on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme ("SWIFT" Agreement)

Introduction

On 27 July 2009, the Council adopted a mandate for the Presidency to negotiate an Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme[1]. This mandate was adopted in view of the imminent "redistribution of the IT architecture" of the provider of international financial payment messaging data, likely to be designated under such future Agreement. SWIFT will move its "European zone" transactions data from its US database to its database in Europe by the end of 2009.

[1] 11724/09 JAI 452 USA 55 RELEX 640 DATAPROTECT 47 ECOFIN 496 RESTREINT UE.

Following the adoption of the negotiation mandate, the Presidency, assisted by the Commission, has held exploratory talks with the US delegation on 29 July and on 26 August 2009. A first round of negotiations with the US delegation (consisting of representatives of the US Treasury, Justice and State Department) took place in Washington DC on 9, 10 and 11 September 2009. A second negotiations round took place in Brussels on 22, 23, 24 and 25 September. Following further negotiation rounds which have been held in Brussels (13-15 October 2009) and Washington DC (2-4 November 2009), the EU and US delegations have reached consensus on a draft agreement. Obviously this consensus is ad referendum, subject to political approval on both sides.

Mutual legal assistance option

The negotiation guidelines that were given to the Presidency by the Council on 27 July 2009 required the Presidency to negotiate an Agreement in which "a public authority [would] be design[at]ed with responsibility to receive requests from the United States Department of the Treasury for financial payment messaging data". Already during the discussions of the negotiation mandate, it transpired that there was no obvious candidate for this "Authority". The Presidency, assisted by the Commission, scrutinised all possible options. Within the short timeframe within which this Agreement had to be negotiated, it was impossible to envisage any legislative change with regard to the powers or status of any such "Authority", whether it is at EU level or at Member State level. Therefore the Presidency has negotiated a draft Agreement, which refers to the existing mutual legal assistance channels and the existing authorities responsible for the mutual legal assistance request. At the JHA Counsellors meeting of 9 November 2009, where various options were discussed, there was consensus surrounding this option.

The mechanism provided for in the draft Agreement set out in Annex II to this note, refers to Article 8 of the EU-US Agreement on mutual legal assistance of 25 June 2003, which will enter into force on 1 February 2010. This Agreement has been implemented at bilateral level between all Member States and the United States of America. The US Treasury Department will, through the US Department of Justice, make requests to the central authority of the Member State where the Designated Provider is based or where it stores its data, which will verify that the request accords with the EU-US Agreement and the applicable requirements of the bilateral mutual legal assistance agreement.

Long-term Agreement

This Agreement is, in accordance with the negotiation guidelines given to the Presidency, a short-term Agreement. It will enter into force on 1 February 2010 (the date of entry into force of EU-US Agreement on mutual legal assistance of 25 June 2003) and expire at the latest on 31 January 2011. Under Article 218 TFEU, the Commission will have to make a recommendation to the Council regarding a long-term Agreement. Several delegations have requested that a declaration be drawn up regarding a European solution for such long-term Agreement. The Presidency will endeavour to draw up such declaration in good time, so that it can be adopted at the same time as the draft Council Decision on signing of this Agreement.

The Presidency has equally taken note of the request that this long-term Agreement be signed in all official languages of the European Union.

Draft Council Decision on signing

Delegations find attached, in Annex I, a draft Council decision on signing, and a draft declaration to be made by the European Union at the time of signing (identical to the declaration made by the European Union at the time of the signing of the 2007 EU-US PNR Agreement).

Further to the outcome of the JHA Counsellors meeting of 9 November 2009, delegations are invited to approve 1) the draft Council Decision on signing set out in Annex I; and 2) the draft EU-US Agreement set out in Annex II, so that these can be subjected to lawyer-linguist scrutiny in time for the adoption on 30 November 2009.

ANNEX I

COUNCIL DECISION (2009/.../CFSP/JHA)

of

between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 24 and 38 thereof,

Whereas:

(1) On 27 July 2009 the Council decided to authorise the Presidency, assisted by the Commission, to open negotiations for an Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme. Those negotiations have been successful and a draft Agreement has been drawn up,

(2) This Agreement is important in ensuring that designated providers of international financial payment messaging services make available to the US Treasury Department financial payment messaging data stored in the territory of the European Union necessary for preventing and combating terrorism and its financing, subject to strict compliance with safeguards on privacy and the protection of personal data,

(3) The Agreement should be signed, subject to its conclusion at a later date,

(4) Article 15 of the Agreement provides that the Agreement will be applied provisionally as of the date of signature. Member States should therefore give effect to its provisions as from that date in conformity with existing domestic law. A declaration to that effect will be made at the time of signature of the Agreement.

HAS DECIDED AS FOLLOWS:

Article 1

The signing of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, is hereby approved on behalf of the European Union, subject to the conclusion of the said Agreement.

The text of the Agreement is attached to this Decision.

Article 2

The President of the Council is hereby authorised to designate the person(s) empowered to sign the Agreement on behalf of the European Union, subject to its conclusion.

Article 3

In accordance with Article 15 of the Agreement, the provisions of the Agreement shall be applied on a provisional basis in conformity with existing domestic law as of the date of its signature, pending its entry into force. The annexed Declaration on provisional application is to be made at the time of signature.

Done at

For the Council

The President

Annex to the ANNEX I

DECLARATION

TO BE MADE ON BEHALF OF THE EUROPEAN UNION

AT THE TIME OF THE SIGNING OF

THE AGREEMENT BETWEEN THE EUROPEAN UNION AND

THE UNITED STATES OF AMERICA

ON THE PROCESSING AND TRANSFER OF FINANCIAL MESSAGING DATA FROM THE EUROPEAN UNION TO THE UNITED STATES FOR PURPOSES OF THE TERRORIST FINANCE TRACKING PROGRAMME

"This Agreement, while not derogating from or amending the legislation of the EU or its Member States, will, pending its entry into force, be implemented provisionally by the Member States in good faith, in the framework of their existing national laws."

ANNEX II

AGREEMENT

between the European Union and the United States of America on the processing and transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program

THE EUROPEAN UNION

and

THE UNITED STATES OF AMERICA ("the Parties"),

1. Desiring to prevent and combat terrorism and its financing, in particular by mutual sharing of information, as a means of protecting their respective democratic societies and common values, rights, and freedoms;

2. Seeking to enhance and encourage cooperation between the Parties in the spirit of transatlantic partnership;

3. Recalling the United Nations conventions for combating terrorism and its firiancing, and relevant resolutions of the United Nations Security Council in the field of fighting terrorism, in particular United Nations Security Council Resolution 1373 (2001);

4. Recognising that the United States Department of the Treasury's ("U.S. Treasury Department") Terrorist Finance Tracking Program ("TFTP") has been instrumental in identifying and capturing terrorists and their financiers and has generated many leads that have been disseminated for counter terrorism purposes to competent authorities around the world, with particular value for European Union Member States ("Member States");

5. Noting the importance of the TFTP in preventing and combating terrorism and its financing in the European Union and elsewhere, and the important role of the European Union in ensuring that designated providers of international financial payment messaging services make available financial payment messaging data stored in the territory of the European Union which is necessary for preventing and combating terrorism and its financing, subject to strict compliance with safeguards on privacy and the protection of personal data;

6. Mindful of Article 6(2) of the Treaty on European Union on respect for fundamental rights, the principles of proportionality and necessity concerning the right to respect for privacy and the protection of personal data under Article 8(2) of the European Convention on the Protection of Human Rights and Fundamental Freedoms, the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union;

7. Stressing the common values governing privacy and the protection of personal data in the European Union and the United States of America ("United States"), including the importance which both Parties assign to due process and the right to seek effective remedies for improper government action;

8. Noting the rigorous controls and safeguards utilised by the U.S. Treasury Department for the handling, use, and dissemination of financial payment messaging data pursuant to the TFTP, as described in the representations of the U.S. Treasury Department published in the Official Journal of the European Union on 20 July 2007 and the Federal Register of the United States on 23 October 2007, which reflect the ongoing cooperation between the United States and the European Union in the fight against global terrorism;

9. Recalling that, to guarantee effective exercise of their rights, any person irrespective of nationality is able to lodge a complaint before an independent data protection authority, other similar authority, independent and impartial court or tribunal, to seek effective remedies;

10. Mindful that appropriate administrative or judicial redress is available under U.S. law for mishandling of personal data, including under the Administrative Procedure Act of 1946 (5 U.S.C. 701 et seq.), the Inspector General Act of 1978 (5 U.S.C. App.), the Implementing Recommendations of the 9/11 Commission Act of 2007 (42 U.S.C. 2000ee et seq.), the Computer Fraud and Abuse Act (18 U.S.C. 1030), and the Freedom of Information Act (5 U.S.C. 552), as amended, among others;

11. Recalling that by law within the European Union customers of financial institutions and of providers of financial payment messaging services are informed that personal data contained in financial transaction records may be transferred to Member States' or third countries' public authorities for law enforcement purposes;

12. Affirming that this Agreement does not constitute a precedent for any future arrangements between the United States and the European Union, or between either of the Parties and any State, regarding the processing and transfer of financial payment messaging data or any other form of data, or regarding data protection;

13. Recognising that this Agreement does not derogate from the existing powers of data protection authorities in Member States to protect individuals with regard to the processing of their personal data; and

14. Further affirming that this Agreement is without prejudice to other law enforcement or information sharing agreements or arrangements between the Parties or between the United States and Member States;

HAVE AGREED AS FOLLOWS:

Article 1 (Purpose of Agreement)

1. The purpose of this Agreement is to ensure, with full respect for the privacy, protection of personal data, and the other conditions set out in this Agreement, that:

(a) financial payment messaging and related data stored in the territory of the European Union by providers of international financial payment messaging services, which are jointly designated pursuant to this Agreement, are made available upon request by the U.S. Treasury Department for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing; and

(b) relevant information obtained through the TFTP is made available to law enforcement, public security, or counter terrorism authorities of Member States, or Europol or Eurojust, for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing.

2. The United States, the European Union, and its Member States shall take all necessary and appropriate measures within their authority to carry out the provisions and achieve the purpose of this Agreement.

Article 2 (Scope of Application – Conduct Pertaining to Terrorism or Terrorist Financing)

This Agreement applies to the obtaining and use of financial payment messaging and related data with a view to the prevention, investigation, detection, or prosecution of:

(a) Acts of a person or entity that involve violence, or are otherwise dangerous to human life or create a risk of damage to property or infrastructure, and which, given their nature and context, are reasonably believed to be committed with the aim of:
   (i) intimidating or coercing a population;
   (ii) intimidating, compelling, or coercing a government or international organization to act or abstain from acting; or
   (iii) seriously destabilizing or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organization;
(b) A person or entity assisting, sponsoring, or providing financial, material, or technological support for, or financial or other services to or in support of, acts described in subparagraph (a); or
(c) A person or entity aiding, abetting, or attempting acts described in subparagraphs (a) or (b).

Article 3 (Ensuring Provision of Data by Designated Providers)

The European Union shall ensure, in accordance with this Agreement, that entities jointly designated by the Parties under this Agreement as providers of international financial payment messaging services ("Designated Providers") make available to the U.S. Treasury Department requested financial payment messaging and related data for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing ("Provided Data").

Article 4 (U.S. Requests to Obtain Data from Designated Providers)

1. Pursuant to Article 8 of the Agreement on Mutual Legal Assistance between the European Union and the United States of America, signed at Washington on 25 June 2003, and related bilateral mutual legal assistance instrument between the United States and the Member State, in which the Designated Provider is either based or where it stores the requested data, the U.S. Treasury Department shall issue a request based on an ongoing investigation concerning a specific conduct referred to in article 2 that has been committed or where there is, based on pre-existing information or evidence, a reason to believe that it could be committed.

2. The request will identify as clearly as possible data stored by a Designated Provider in the territory of the European Union which is necessary to this end. Data may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national identification number, and other personal data.

The request shall substantiate the necessity for the data and shall be tailored as narrowly as possible in order to minimize the amount of data requested, taking due account of geographic, threat and vulnerability analyses.

3. The request shall be transmitted by the U.S. Department of Justice to the central authority of the Member State in which the Designated Provider is based or where it stores the requested data.

4. The U.S. Department of Justice shall simultaneously transmit a copy of the request to the central authority of the other Member State. The U.S. Department of Justice shall also simultaneously transmit a copy of the request to national members of Eurojust of these member States.

5. On receipt of the substantiated request in accordance with paragraph 3, the central authority of the requested State shall verify the admissibility of the request according to this Agreement and the requirements of the bilateral mutual legal assistance agreement. Where the central authority has so verified, the request shall be transmitted to the competent authority for its execution under the law of the requested State.

If the request has been transmitted to the central authority of the Member State in which the Designated Provider is based the Member State where the data are stored shall give assistance to the execution of the request.

The requested measure shall be executed as a matter of urgency.

6. If the Designated Provider is not able to identify the data that would respond to the request because of technical reasons, all potentially relevant data shall be transmitted in bulk to the competent authority of the requested State.

7. The data shall be transferred between the designated authorities of the requested State and of the US.

8. The EU shall ensure that Designated Providers keep a detailed log of all data transmitted to the competent authority of the requested State for the purpose of this Agreement.

9. The data that have been transmitted lawfully on the basis of this provision may be searched for the purpose of other investigations concerning the same type of conducts, with full respect of article 5 of this Agreement.

Article 5 (Safeguards Applicable to the Processing of Provided Data)

1. The U.S. Treasury Department shall ensure that Provided Data are processed in accordance with the provisions of this Agreement.

2. The TFTP does not involve data mining or any other type of algorithmic or automated profiling or computer filtering. The U.S. Treasury Department shall ensure the protection of personal data by means of the following safeguards, which shall be applied without discrimination, in particular on the basis of nationality or country of residence:

(a) Provided Data shall be processed exclusively for the prevention, investigation, detection, or prosecution of terrorism or its financing;

(b) All searches of Provided Data shall be based upon pre-existing information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing;

(c) Each individual TFTP search of Provided Data shall be narrowly tailored, shall demonstrate a reason to believe that the subject of the search has a nexus to terrorism or its financing, and shall be logged, including such nexus to terrorism or its financing required to initiate the search;

(d) Provided Data shall be maintained in a secure physical environment, stored separately from any other data, with high-level systems and physical intrusion controls to prevent unauthorized access to the data;

(e) Access to Provided Data shall be limited to analysts investigating terrorism or its financing and to persons involved in the technical support, management, and oversight of the TFTP;

(f) No copies of Provided Data shall be made, other than for disaster recovery back-up purposes;

(g) Provided Data shall not be subject to any manipulation, alteration, or addition and shall not be interconnected with any other database;

(h) Information obtained through this Agreement shall only be shared with law enforcement, public security, or counter terrorism authorities in the United States, European Union, or third states to be used for the purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing;

(i) During the term of this Agreement, the U.S. Treasury Department shall undertake a review to identify all non-extracted data that are no longer necessary to combat terrorism or its financing. Where such data are identified, procedures to delete those data shall commence within two months of the date that they are so identified and shall be completed as soon as possible thereafter but in any event no later than 8 months after identification, absent extraordinary technological circumstances;

(j) If it transpires that financial payment messaging data were transmitted which were not requested, the U.S. Treasury Department shall promptly and permanently delete such data and shall inform the relevant Designated Provider and central authority of the requested Member State;

(k) Subject to subparagraph (i), all non-extracted data received prior to 20 July 2007 shall be deleted not later than five years after that date;

(l) Subject to subparagraph (i), all non-extracted data received on or after 20 July 2007 shall be deleted not later than five years from receipt; and

(m) Information extracted from Provided Data, including information shared under subparagraph (h), shall be subject to the retention period applicable to the particular government authority according to its particular regulations and record retention schedules.

Article 6 (Adequacy)

Subject to ongoing compliance with the commitments on privacy and protection of personal data set out in this Agreement, the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the processing of financial payment messaging and related data transferred from the European Union to the United States for purposes of this Agreement.

Article 7 (Spontaneous Provision of Information)

1. The U.S. Treasury Department shall ensure the availability, as soon as practicable, to law enforcement, public security, or counter terrorism authorities of concerned Member States, and, as appropriate, to Europol within the remit of its mandate, of information obtained through the TFTP that may contribute to the investigation, prevention, detection, or prosecution in the European Union of terrorism or its financing. Any follow-on information that may contribute to the investigation, prevention, detection, or prosecution in the United States of terrorism or its financing shall be conveyed back to the United States on a reciprocal basis.

2. In order to facilitate the efficient exchange of information, Europol may designate a liaison officer to the U.S. Treasury Department. The modalities of the liaison officer's status and tasks shall be decided jointly by the Parties.

Article 8 (EU Requests for TFTP Searches)

Where a law enforcement, public security, or counter terrorism authority of a Member State, or Europol or Eurojust, determines that there is reason to believe that a person or entity has a nexus to terrorism as defined in Articles 1 to 4 of Council Framework Decision 2002/475/JHA as amended by Council Framework Decision 2008/919/JHA, such authority may request a search for relevant information obtained through the TFTP. The U.S. Treasury Department shall promptly conduct a search in accordance with Article 5 and provide relevant information in response to such requests.

Article 9 (Cooperation with Future Equivalent EU System)

In the event that an EU system equivalent to the U.S. TFTP is implemented in the European Union or in one or more of its Member States that requires financial payment messaging data stored in the United States to be made available in the European Union, the U.S. Treasury Department shall actively pursue, on the basis of reciprocity and appropriate safeguards, the cooperation of any relevant international financial payment messaging service providers which are based in the territory of the United States.

Article 10 (Joint Review)

1. The Parties shall jointly review, after a period of six months, the implementation of this Agreement with particular regard to verifying the privacy, protection of personal data, and reciprocity provisions set out in this Agreement. The review shall include a proportionality assessment of the Provided Data, based on the value of such data for the investigation, prevention, detection, or prosecution of terrorism or its financing.

2. In the review, the European Union shall be represented by the Presidency of the Council of the European Union, the European Commission, and two representatives of data protection authorities from Member States at least one of which shall be from a Member State where a Designated Provider is based. The United States shall be represented by the U.S. Treasury Department.

3. For purposes of the review, the U.S. Treasury Department shall ensure access to relevant documentation, systems, and personnel, as well as precise data relating to the number of financial payment messages accessed and the number of occasions on which leads have been shared. The Parties shall jointly determine the modalities of the review.

Article 11 (Redress)

1. Any person has the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay or expense, confirmation from his or her data protection authority whether all necessary verifications have taken place within the European Union to ensure that his or her data protection rights have been respected in compliance with this Agreement, and, in particular, whether any processing of his or her personal data has taken place in breach of this Agreement. Such right may be subject to necessary and proportionate measures applicable under national law, including for the protection of public security or national security or to avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences, with due regard for the legitimate interest of the person concerned.

2. The Parties shall take all reasonable steps to ensure that the U.S. Treasury Department and any relevant Member State promptly inform one another, and consult with one another and the Parties, if necessary, where they consider that personal data have been processed in breach of this Agreement.

3. Any person who considers his or her personal data to have been processed in breach of this Agreement is entitled to seek effective administrative and judicial redress in accordance with the laws of the European Union, its Member States, and the United States, respectively.

Article 12 (Consultation)

1. The Parties shall, as appropriate, consult to enable the most effective use to be made of this Agreement, including to facilitate the resolution of any dispute regarding the interpretation or application of this Agreement.

2. The Parties shall take measures to avoid the imposition of extraordinary burdens on one another through application of this Agreement. Where extraordinary burdens nonetheless result, the Parties shall immediately consult with a view to facilitating the application of this Agreement, including the taking of such measures as may be required to reduce pending and future burdens.

3. The Parties shall immediately consult in the event any third party, including an authority of another country, challenges or asserts a legal claim with respect to any aspect of the effect or implementation of this Agreement.

Article 13 (Non-derogation)

This Agreement is not intended to derogate from or amend the laws of the United States or the European Union or its Member States. This Agreement does not create or confer any right or benefit on any other person or entity, private or public.

Article 14 (Termination)

1. Either party may terminate this Agreement at any time by notification through diplomatic channels. Termination shall take effect thirty (30) days from the date of receipt of such notification.

2. Notwithstanding the termination of this Agreement, all data held by the U.S. Treasury Department pursuant to this Agreement shall continue to be processed in accordance with this Agreement.

Article 15 (Final Provisions)

1. This Agreement shall enter into force on the first day of the month after the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for this purpose.

2. This Agreement shall apply provisionally from 1 February 2010, until its entry into force, subject to paragraph 3.

3. Unless previously terminated in accordance with Article 14 or by agreement of the Parties, this Agreement shall expire and cease to have effect not later than 31 January 2011.

4. As soon as the Treaty of Lisbon enters into force, the Parties shall endeavour to conclude a long-term agreement to succeed this Agreement.

5. Done at Brussels this xxxx day of xxxx 2009, in two originals, in the English language. It shall also be drawn up in the Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish, and Swedish languages. Upon approval by both Parties, these language versions shall be considered equally authentic.

[redacted]

COUNCIL OF THE EUROPEAN UNION

Brussels, 10 November 2009

15671/09
ADD 1

RESTREINT UE

JAI 813
USA 99
RELEX 1043
DATAPROTECT 71
ECOFIN 719

ADDENDUM TO NOTE

from :	Presidency
to :	Delegations
prev.doc.:	15397/09 JAI 782 USA 95 RELEX 1009 DATAPROTECT 69 ECOFIN 699
Subject :	Draft Council Decision on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme ("SWIFT" Agreement)

Delegations find attached a matrix provided by the United States, which explains the redress mechanisms available under US law, referred to in recital 10 of the draft EU-US Agreement.

Presented below is an illustrative, non-comprehensive list of U.S. statutes and regulations that support privacy and the protection of personal data. In particular, they provide mechanisms for administrative and/or judicial redress and access that are available to all persons, regardless of nationality. As a general matter, a workshop was held in Brussels on 1 October 2009 among experts on privacy and personal data protection from the U.S. Government, the EU Presidency, the Commission, several EU Member States, the European Data Protection Supervisor, and the Europol Joint Supervisory Board. The workshop provided an opportunity to enhance mutual understanding of the U.S. and EU frameworks for redress in the context of law enforcement. An important conclusion was that while the legal systems, traditions and government structures in the U.S. and EU differ, both jurisdictions provide multiple mechanisms for administrative and judicial redress.

Statute/Regulation	Description
Administrative Procedure Act of 1946, 5 U.S.C. 701 et seq.	The Administrative Procedure Act ("APA") provides that a person who suffers legal wrong as a result of agency action, or is otherwise adversely affected or aggrieved by agency action within the meaning of a relevant statute, may seek judicial review of the action. The APA also sets forth criteria pursuant to which agency action may be compelled or found unlawful and set aside by a reviewing court.
Inspector General Act of 1978, 5 U.S.C. App.	The Act empowers inspectors general of federal agencies to audit and investigate agency programs and operations, and to report to the heads of such agencies and Congress concerning fraud and other serious problems, abuses, and deficiencies relating to the administration of agency programs and operations.

Statute/Regulation	Description
Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. 2000ee et seq.	The Act establishes an independent "Privacy and Civil Liberties Oversight Board" in the executive branch of the U.S. government. The Board is charged with reviewing laws, regulations, policies, and guidelines related to counterterrorism efforts, and advising the President and executive branch agencies to ensure that privacy and civil liberties are appropriately considered in the development and implementation of such laws, regulations, policies, and guidelines. The Act requires executive branch agencies to designate privacy and civil liberties officers to provide advice, oversight, and reporting regarding the impact on privacy and civil liberties of counterterrorism laws, regulations, and policies. It also ensures that agencies have a Chief Privacy Officer to assume primary responsibility for privacy and data protection policy, and requires agencies to establish and implement comprehensive privacy and data protection procedures governing the agencies' collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to their employees and the public.
Computer Fraud and Abuse Act, 18 U.S.C. 1030 (criminal)	The Act criminalizes intentional access, without or in excess of authorization, to obtain information from a financial institution, a U.S. government computer system, or a computer accessed via the Internet affecting interstate or foreign commerce or communication. It also criminalizes trafficking in passwords for unauthorized access to defraud and threatening to damage protected computers for purposes of extortion.

Statute/Regulation	Description
Computer Fraud and Abuse Act, 18 U.S.C. 1030(g) (civil)	Any person who suffers damage or loss by reason of a violation of this Act may maintain a civil action against the violator (including a government official) to obtain compensatory damages and injunctive or other equitable relief under 18 U.S.C. § 1030(g), regardless of whether a criminal prosecution has been pursued, provided the conduct involves at least one of several circumstances set forth in the statute.
Freedom of Information Act (FOIA), 5 U.S.C. 552	FOIA allows individuals access to records about them (with a few exceptions) maintained by or for any USG agency. If the requester is unsatisfied with the Agency's response, he or she is entitled to challenge the decision first through an administrative appeal process, and then via federal court up to and including the U.S. Supreme Court. The requester may also recover attorney's fees.
Title 5 of C.F.R., Chapter XVI, Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch	This Code establishes standards of ethical conduct for employees of executive agencies of the U.S. government. Sec. 101 Employees are required to protect and conserve federal property and are not to use it for other than authorized activities. Sec. 703 Employees are prohibited from improperly using non public information to further private interests. An agency may take administrative action against an employee who violates these provisions; such action may range from a letter of reprimand to suspension from work without pay to removal from federal office.