EUROPEAN PARLIAMENT
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Data Protection in a Transatlantic Perspective: Future EU-US international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters.

Marc ROTENBERG, President
Electronic Privacy Information Center ("EPIC")

Brussels, Belgium
26 October 2010

A. Introduction

- On behalf of EPIC I would like to thank the Committee for the invitation to this hearing regarding data protection in a transatlantic perspective/EU-US agreement in the framework of police and judicial cooperation in criminal matters.

- I will specifically address the shared values, constitutional constraints and possible common solutions ensuring proportionality, judicial review and independent and effective oversight of Council Framework Decision 2008/977/JHA

- EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a leading civil liberties organization that has reported on developments in privacy and human rights around the world for several years.

B. Data Protection Directive/Council Framework Decision 2008/977/JHA

- The Data Protection Directive of 1995 applies to all personal data processing activities in EU Member States in both public and the private sector but not to the processing of personal data by police and judicial authorities in criminal matters.

- The Council Framework is the first horizontal data protection instrument in the field of personal data used by police and judicial authorities in the EU and its main purpose is to establish a common level of privacy protection and a high level of security when exchanging personal data.

- These two instruments are complemented by other EU instruments such as Regulation (EC) n° 45/2001 regulating the processing of personal data by EU

institutions and bodies and by Directive 2002/58/EC on privacy and electronic communications ("e-Privacy" Directive).

- The Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, has recognized that the Council Framework cannot be considered to ensure a level of protection equivalent to that offered by the Data Protection Directive and does not achieve consistency with other EU legal instruments. The Council of Europe has not adopted the EU Parliament recommendations such as references to Convention 108.

- EPIC strongly supports full implementation of the EU Data Directive as well as other efforts to fully safeguard the fundamental rights of citizens, consumers, and users of Internet-based services. This principles should apply to data collection that occurs by both private and public entities.

- EPIC also supports Council of Europe Convention 108 and has launched a campaign urging the US Government to support the Council of Europe Privacy Convention. Thirty distinguished members of the EPIC Advisory Board have urged US Secretary of State Hilary Clinton to begin the process of US ratification of COE 108

- And EPIC has supported the Madrid Privacy Declaration (2009), created by civil society and endorsed by hundreds of experts in the field on privacy and data protection.

- The European Parliament and the Council of Europe shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data.

- The Framework Decision must protect the fundamental rights and freedoms of natural persons when their personal data are processed for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. It concerns personal data that are processed in part or entirely by automatic means, as well as personal data forming part of a filing system that are processed by non-automatic means.

- The Framework Decision is applicable to cross-border exchanges of personal data within the framework of police and judicial cooperation. The instrument contains rules applicable to onward transfers of personal data to third countries, such as the US, and to the transmission to private parties in Member States. The Framework Decision encourages the EU states to have higher-level safeguards for protecting personal data.

- However, the Framework Decision does not apply to Member State domestic data. The Framework Decision indeed only covers police and judicial data exchanged between Member States, EU authorities and systems, which explicitly excludes exchanges such as the transfer of Passenger Name Records (PNR) data to third countries such as US authorities.

C. <u>US Protection to EU Citizens</u>

- As a general proposition, we reject the proposition that police agencies can investigate people and compel disclosure of private information --absent a reasonable indication of criminal activity. The Fourth Amendment of the US Constitution requirements of probable cause of a crime, supported by the judicial issuance of a warrant, is a bedrock principle of the American system of justice. Unless the government can demonstrate that it has a criminal predicate -- evidenced by a court order or a grand jury subpoena -- the government should not be given access to sensitive or private information about individuals even if that information is maintained by third parties.

- Proposals that would require disclosure of information for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism should be adopted only if it is certain that the information is provided within the context of a legal framework that ensures accountability a nd prevents the use of the information in other context that may violate the privacy rights of individuals.

- Although the US has no general privacy law, the Privacy Act of 1974 provides a comprehensive legal framework that regulates the collection, maintenance, use and dissemination of personal information by federal executive branch agencies. There are clear penalties in the act for violations; however, enforcement is often unclear as there is no privacy agency in the United States responsible for administration, and those seeking to enforce rights under the Privacy Act must often find a private attorney and bring an action in court.

- According to the Privacy Act, in order to start a civil action against an agency, the behavior of the agency must have had an adverse effect on the individual. This can be a difficult showing for an individual to make, even though the agency violation may have had an impact on thousands, or millions, of individuals.

- Under the Privacy Act, "individuals" who have data protection rights are defined as citizens of the United States or aliens lawfully admitted for permanent residence, which excludes visitors or aliens.

- However, non-US citizens or legal residents do not enjoy the right to judicial redress, i.e. to have the lawfulness of the processing of his or her personal data assessed by an independent, judicial authority. In contrast, EU law asserts that every individual in the EU has the right to redress before an impartial and

independent tribunal regardless of his or her nationality or place of residence.

- As an example, on January 2009, the policy of the Department of Homeland Security Privacy Office has been amended with the effect that "any personally identifiable information that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.' Moreover, it is indicated that "[u]nder this policy, DHS components will handle non-U.S. person personally identifiable information held in mixed systems in accordance with the fair information practices, as set forth in the Privacy Act."

- Non-U.S. persons have the right of access to their personally identifiable information and the right to amend their records, absent an exemption under the Privacy Act. However, this policy does not extend or create a right of judicial review for non-U.S. persons.

- Furthermore, personal data of non-US individuals not held in 'mixed-systems' (i.e. systems of records containing personal data on both US and non-US citizens), but in systems of records, which only relate to foreigners (such as the US-ESTA) are not protected and not covered by this policy.

- While no U.S. law currently requires DHS to protect the privacy of non-U.S. citizens as the agency develops and deploys US-VISIT, EPIC has urged the DHS to consider the application of international privacy standards to the collection and use of personal information obtained for non-U.S. citizens. The international community has recognized time and time again that all individuals have rights in their personal information, regardless of nationality.

- Furthermore, other US privacy laws, such as the Computer Fraud and Abuse Act, the Wire and Electronic Communications Interception and Interception of Oral Communications, the Video Privacy Protection Act and the subscriber privacy provisions in the Cable Act provide recourse for an aggrieved individual to file a civil action in US federal court for damages and make no distinction based on citizenship.

- Stated most simply, there is no necessary reason that US privacy could not extend the same rights to non-US citizens as it does to US-citizens. The US Congress has done so in the past and could do so in the future. Nor is there any obvious reason that a court would disfavor such a law.

- The Universal Declaration of Human Rights provides that no individual "shall be subjected to arbitrary interference with his privacy," and that "[e]veryone has the right to protection of the law against such interference or attacks."

- Furthermore, "no distinction shall be made on the basis of the political,

jurisdictional, or international status of the country or territory to which a person belongs". The United States was a key architect of the Universal Declaration and one of the original signatories. It is thus surprising to find our nation deploying a system that violates the Universal Declaration by encroaching upon the privacy of individuals based on their lack of U.S. citizenship, and failing to provide them rights in their personal information held by the United States. By neglecting to give non-U.S. citizens rights in information about them used in the US-VISIT program, the United States has failed to comply with this widely recognized legal regime for privacy protection.

- We believe EU citizens must be protected by the US Privacy Act on the sharing of transatlantic personal data with regard to redress and compensation. Judicial review and effective oversight of this process are critical elements.

D. Recommendations for EU-US International Agreement

- The EU-US data protection agreement must set out which data can be shared with the US for law enforcement purposes exclusively. The agreement must aim to provide legal certainty and a set of clearly defined rights for EU citizens, such as the possibility to file complaints about misused data. EU citizens' complaints should be handled in the same manner as American citizens in US courts.

- To respond to the latest technological developments and to integrate in a coherent way the already existing data protection instruments in the area of police and judicial cooperation in criminal matters it is necessary that EU legal frameworks share the same values as the US for data protection privacy.

- The same data protection principles should apply – no matter whether individual's data is processed for commercial or public enforcement principles.

- It is important to ensure that any citizen will still receive a fair trial if this occurs. The Framework Decision must extend privacy as a safeguard to personal data that is transferred outside the European Union such as the Data Protection Directive does.

- Personal data must only be collected for specified, explicit and legitimate purposes. The processing of these data must only be permitted for the purposes for which they were collected. Processing for other purposes can only be allowed when certain appropriate safeguards are in place.

- Inaccurate personal data must be rectified and updated or completed if possible. Once the data is no longer needed for the purposes they were collected, they must be erased, made anonymous or, in certain cases, blocked. The need to store personal data must be reviewed regularly, with time limits set for their erasure.

- Member States must verify that the personal data to be transmitted or made

available to other Member States or the US are accurate, up to date and complete. In order to be able to verify that the processing of data is lawful and to ensure the integrity and security of the data, their transmissions must be logged or documented.

- Personal data received from another Member State or from the US are to be processed only for the purposes for which they were transmitted. The receiving Member State must respect any specific restrictions to the exchanges of data provided for in the law of the transmitting Member State or from the US.

- The data subject is to be kept informed of any collection or processing of personal data relating to him/her. However, when data has been transmitted from one Member State to another or third countries, the first may demand that the second does not divulge any information to the subject.

- The data subject may request to receive a confirmation on whether data concerning him/her have been transmitted, who the recipients are, what data are being processed, as well as a confirmation that the necessary verifications of that data have been made. In certain cases, Member States may restrict the subject's access to information. Any decision restricting access must be given in writing to the data subject, together with the factual and legal reasons thereof. The data subject must also be given advice on his/her right to appeal such a decision.

- The data subject may demand that personal data relating to him/her be rectified, erased or blocked. Any refusal to that end must be given in writing, along with information on the right to lodge a complaint or seek a judicial remedy.

- Any person may demand compensation for the damages s/he has suffered due to an unlawful processing of personal data or any other act that is not compatible with this Framework Decision. In case a data subject's rights are breeched, s/he has the right to a judicial remedy.

- The competent authorities must take the necessary security measures to protect personal data against any unlawful form of processing. This includes accidental loss, alteration and unauthorized disclosure of, as well as access to, personal data. In particular, specific measures need to be taken with regard to the automated processing of data.

- National supervisory authorities in Member States and the US must have investigative powers, effective powers of intervention, as well as the power to pursue legal proceedings. For any infringements of the provisions of this Framework Decision, Member States must establish effective, proportionate and dissuasive penalties.