COUNCIL OF THE EUROPEAN UNION

Brussels, 28 May 2008

9831/08

LIMITE

JAI 275
DATAPROTECT 31
USA 26

NOTE

from :	Presidency
to :	COREPER
Subject :	EU US Summit, 12 June 2008 - Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection

Following the EU US Ministerial Troika of 12-13 March 2008, the Presidency announced it would keep Coreper informed of the work of the High Level Contact Group.

The Presidency is pleased to announce that the EU-US High Level Contact Group on information sharing and privacy and personal data protection has now finalised its report, which the HLCG intends to submit to the EU-US Summit of 12 June 2008.

The Presidency would like to highlight that this draft final report as such is not a report by the Council or by the European Union, but by the High Level Contact Group. In this perspective, there is no scope for amending this report, but the Presidency would welcome any ideas with regard to the follow-up to this report, and in particular reactions to the recommendations on the ways forward identified in the report.

Draft Final Report by the EU-U.S. High Level Contact Group
on information sharing and privacy and personal data protection

1. INTRODUCTION: CONTEXT AND BACKGROUND

In the framework of the EU-U.S. JLS Ministerial Troika on 6 November 2006, it was decided to establish an informal high level advisory group to start discussions on privacy and personal data protection in the context of the exchange of information for law enforcement purposes as part of a wider reflection between the EU and the U.S. on how best to prevent and fight terrorism and serious transnational crime. This group is composed of senior officials from the Commission, the Council Presidency (supported by the Council Secretariat) and the U.S. Departments of Justice, Homeland Security and State. The goal of the HLCG was to explore ways that would enable the EU and the U.S. to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. The group's identification of the fundamentals or "common principles" of an effective regime for privacy and personal data protection was to be the first step towards that goal.

This goal builds on recent trans-atlantic events in the Justice and Home Affairs area, which have included the conclusion of international agreements between the United States and the European Union governing Extradition and Mutual Legal Assistance (2003), and Passenger Name Record (PNR) data (2007), as well as agreements governing personal data exchange between the United States and Europol (2002) and Eurojust (2006).

U.S. and EU Ministers responsible for Justice and Home Affairs directed the HLCG to explore the commonalities of these agreements, as well as our laws, policies and practices, and the potential efficiencies that could result from the development of common principles.

At its first meeting on 26 February 2007 in Washington, the group began work to identify and define a set of core principles on privacy and personal data protection, acceptable as minimum standards when processing personal data for law enforcement purposes. At that meeting the group identified a set of core privacy and personal data protection principles and a set of related implementing principles, and decided to establish an informal experts group to begin the task of developing agreed definitions of these principles. It was understood that the HLCG would also report, when appropriate, to the EU-U.S. JLS Ministerial Troika.

At the EU-U.S. JLS Ministerial Troika in Berlin on 4/5 April 2007, the experts were asked to continue their discussions.

At its third meeting on 2 November 2007 in Washington, the HLCG concluded that good progress had been made and decided that the experts should continue the exploratory talks with the aim of trying to find as much common ground as possible by the end of 2007.

At the EU-U.S. JLS Ministerial Troika in Brdo on 12/13 March 2008, Ministers expressed a clear common will to continue working on the principles, to identify options for future work and to report on any outstanding issues. It was also said that such reporting could take place in the context of the EU-U.S. Summit in June 2008. This report seeks to fulfil that commitment.

2. CURRENT STATE OF PLAY

A. Scope

The HLCG discussed the scope of the principles under consideration and agreed that the principles set forth below would, if put into some operational form, apply to information exchanges made for a law enforcement purpose. Specifically:

> The European Union would apply these principles for "law enforcement purposes", meaning use for the prevention, detection, investigation or prosecution of any criminal offense.

The United States would apply these principles for 'law enforcement purposes', meaning for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations.

These two different ways of describing 'law enforcement purposes' reflect respective domestic legislation and history but may in practice coincide to a large extent.

B. Agreed upon principles

These principles, the text of which is attached as an annex to this report, define the following privacy and personal data protection requirements:

1. Purpose Specification/Purpose Limitation;
2. Integrity/Data Quality;
3. Relevant and Necessary/Proportionality;
4. Information Security;
5. Special Categories of Personal Information (sensitive data);
6. Accountability;
7. Independent and Effective Oversight;
8. Individual Access and Rectification;
9. Transparency and Notice;
10. Redress;[1]
11. Automated Individual Decisions;
12. Restrictions on Onward Transfers to Third Countries.

In order to better understand the scope of application of the principles the following understandings should be specified:

[1] Both the US and EU maintain a reservation on this principle as discussed in section 2.C below.

On principle 7 of Independent and Effective Oversight, the principle is drafted to focus on the desired effect - maintaining accountability - irrespective of the constitutionally defined structure of government in the US and Europe. It recognizes both European law, which defines effective and independent supervision as meaning a public data protection supervisory authority, exercising its functions with complete independence from government under EU law, as well as U.S. law, which encompasses a networked and layered system of oversight in the United States.[1]

Principle 9 of Transparency and Notice identifies the information that should be made available to data subjects so they can make informed decisions about their actions. In the U.S. this may include, individually or in combination, publication in the Federal Register, individual notice, and disclosure in court proceedings. In other circumstances and as required by law, U.S. Government agencies do inform each individual from whom an agency seeks information. In the EU it is understood that an individual should have an enforceable right to be informed in an appropriate way by the designated authorities of the Member State that personal data could be or are being collected, processed or transmitted; the modalities of the right of the data subject to be informed and the possible limitations thereto shall be determined by national law.

C. Outstanding Issue: Redress

One difference remains concerning the redress principle. Both sides did agree that the key to this principle is to provide the data subject with an effective remedy as a result of any redress process. To date, the HLCG agreed on common language emphasizing the need to make redress available to aggrieved data subjects and what types of actions constitute effective redress if a data subject's claim is found valid. However, disagreement remains over the necessary scope of judicial redress. The EU side 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, whereas the United States recognizes that some laws treat nationals differently.

[1] Both sides prepared and exchanged papers that explained their systems for oversight and accountability.

As the U.S. side has explained, the U.S. framework for privacy protection comes from a networked and layered set of authorities arising from the common law and specific protections guaranteed under the U.S. Constitution. U.S. jurisprudence has long recognized that an individual may seek redress in relation to individual privacy; however, the exercise of that prerogative may be directed or controlled as consistent with the U.S. Constitution.

As such, an individual may generally challenge government actions, including the handling of personal information, before a judicial tribunal, but such government actions must represent final agency decisions affecting a right or benefit of the person. This requirement flows from the separation of powers doctrine of the U.S. Constitution as articulated specifically in the Administrative Procedures Act requiring an individual to exhaust all agency remedies before applying to a court. In this manner, the U.S. legal system permits agency processes to provide redress for agency actions.

Notwithstanding this general procedural requirement, U.S. law does provide exceptions from the general rule through specific authorities, such as the U.S. Freedom of Information Act of 1966 (FOIA) and the U.S. Privacy Act of 1974. Further, the law may define which classes of individuals may take advantage of such exceptions. For example, while the U.S. (FOIA) provides judicial redress to any individual seeking information about himself, the Privacy Act of 1974 limits judicial redress to U.S. citizens and legal permanent residents.

Nonetheless, any individual may seek redress concerning the government handling of personal information through agency administrative redress and may have their case heard in court under appropriate legal grounds other than the Privacy Act. The U.S. side allows that although redress through these alternative means is more attenuated than through the Privacy Act, it still reflects real and operative redress because it ensures the availability of "appropriate and effective sanctions and/or remedies" as defined in this principle. This differs from the position of the EU side which maintains that citizens of EU member states require the ability to bring suit in U.S. courts specifically under the Privacy Act for an agreement to be reached on redress.

3. OUTSTANDING ISSUES PERTINENT TO TRANSATLANTIC RELATIONS

The HLCG identified the following issues as matters pertinent to the transatlantic relationship on privacy, personal data protection and information sharing, and recommends that these be specifically addressed in the final product resulting from the HLCG's work, regardless of whether it is binding or non-binding:

1. Consistency in private entities' obligations during data transfers;
2. Equivalent and reciprocal application of privacy and personal data protection law;
3. Preventing undue impact on relations with third countries;
4. Specific agreements regulating information exchanges and privacy and personal data protection; and
5. Issues related to the institutional framework of the EU and US.

These issues were identified during recent transatlantic discussions over privacy and personal data protection but are not addressed by the 12 principles identified above. They would relate to the possible impacts on the various public and private actors participating in or affected by international data transfers. The EU and U.S. provided text to further describe and explain some of these issues; however, the HLCG did not yet extensively explore this text. Appropriately addressed, these issues could contribute to future transatlantic debate or negotiation over privacy and personal data protection in law enforcement matters

4. POSSIBLE WAYS FORWARD

The HLCG identified the following two main options as possible ways forward:
(i) a binding international agreement or
(ii) non-binding instruments including 'soft law' and a political declaration.

A. Binding international agreement

Both sides agree that an international agreement binding both the EU and the US to apply the agreed common principles in transatlantic data transfers is the preferred option. In negotiating a binding international agreement the EU and US should strive to obtain the recognition of the effectiveness of each other's privacy and data protection systems for the areas covered by these principles. In addition to the agreed common principles, further work could be undertaken to identify detailed key issues to be addressed in such an agreement. Whilst it is difficult/impossible to envisage an international agreement covering all types of law enforcement data, a binding international agreement would offer the advantage of establishing the fundamentals of effective privacy and personal data protection for use in any future agreements relating to the exchange of specific law enforcement information that might arise between the EU and the U.S. As a binding instrument, it would provide the greatest level of legal security and certainty.

Both sides also agree that the conclusion of a binding international agreement incorporating the common principles should provide every person in the EU and the U.S. with the greatest reassurance that her or his personal data would be protected consistently and evenly at a high standard in both jurisdictions.

— Specific considerations for the EU

Political endorsement from the Council would be needed before the Commission could engage in this process, following discussions with EU Member States on the basis of this report. Information and transparency with the European Parliament would need to be ensured.

Political endorsement would mean that the Council considers the results so far achieved as a sufficient basis to prepare formal negotiations. However, it is very likely that the negotiations would need to go beyond the issues addressed by the common principles.

Assuming that the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (Lisbon Treaty) enters into force in the beginning of 2009, it would not be appropriate to start such a process in 2008 under the current legal framework: the negotiation mandate would lapse by the entry into force of the Lisbon Treaty. The negotiating procedure pursuant to Article 218 of the Lisbon Treaty would commence only then. As a consequence the European Parliament would have to be immediately and fully informed at all stages of the procedure, its consent to conclusion of the agreement would be required, and judicial review before the European Court of Justice would be available. This, however, should not preclude additional preparatory work by the HLCG in view of possible negotiations in 2009.

— Specific considerations for the U.S.

Once agreement is confirmed at political level on the common principles, the U.S. departments participating in the HLCG process (State, Justice and Homeland Security) would seek from the Department of State the authority to pursue negotiation of an international agreement. Such an authorization would empower both negotiation and, if so chosen, signature as well.

Further exploratory talks between the two sides would help to establish whether any resulting international agreement could be applied pursuant to existing U.S. laws, including those related to privacy, or would require additional implementing legislation. This would be determinative of the question whether, as a matter of U.S. domestic law, an international agreement could be considered either as an executive agreement entered into by the President or a treaty requiring the advice and consent of the U.S. Senate prior to ratification.

B. Non-binding instruments – "soft law" or a political declaration

Another option is a non-binding instrument but it would provide less certainty and transparency regarding the treatment of personal data. Therefore, such a solution would be less desirable for the long term.

— Specific considerations for the EU

Soft law, such as a non-binding instrument that embodied the "common principles", could be used as a possible reference.

In terms of timing, this option might need the involvement of a wider circle of stakeholders, and could thus be a long process.

Another way forward would be a political declaration reaffirming the importance that both, the EU and the U.S., attach to enhancing the exchange of law enforcement information and to ensuring the mutual respect for the protection of privacy and personal data.

Under both scenarios, political endorsement by the Council would be needed before the EU could engage in this process, following discussions with EU Member States on the basis of the final report. Information of and transparency with the European Parliament would need to be ensured.

— Specific considerations for the U.S.

These non-binding options could serve as a basis for the protection of privacy and personal data, when exchanged for law enforcement purposes as defined above, and may be useful in the short term. These non-binding options could also contribute to the recognition of the effectiveness of each other's privacy and data protection systems for the areas covered by these principles.

If the common principles are not transformed into an international agreement, but instead are utilized in another form, the considerations noted above relating to the U.S. legal process would not be applicable.

5. Conclusion

We recognize that the fight against transnational crime and terrorism requires the ability to share personal data for law enforcement purposes while fully protecting the fundamental rights and civil liberties of our citizens, in particular their privacy and personal data protection, by maintaining necessary standards of personal data protection. Our ongoing discussions of U.S. and European Union frameworks for the protection of personal data have allowed us to identify a number of significant commonalities in our approaches based upon our shared values. The best way to ensure these interests are met is through a binding international agreement that addresses all the issues identified in this report. Our challenge moving forward will be to translate insights into greater collaboration in all aspects of law enforcement cooperation.

Annex: Principles on Privacy and Personal Data Protection for Law Enforcement Purposes for which common language has been developed (common principles)

The European Union would apply these principles for 'law enforcement purposes' meaning use for the prevention, detection, investigation, or prosecution of any criminal offense.

The United States would apply these principles for 'law enforcement purpose,' meaning use for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations.

1. Purpose Specification/Purpose Limitation.

Personal information [should/shall] be processed for specific legitimate law enforcement purposes in accordance with the law and subsequently processed only insofar as this is not incompatible with the law enforcement purpose of the original collection of the personal information.

2. Integrity/Data Quality.

Personal information should be maintained with such accuracy, relevance, timeliness and completeness as is necessary for lawful processing.

3. Relevant and Necessary/Proportionality.

Personal information may only be processed to the extent it is relevant, necessary and appropriate to accomplish a law enforcement purpose laid down by law.

4. Information Security.

Personal information must be protected by all appropriate technical, security and organizational procedures and measures to guard against such risks as loss; corruption; misuse; unauthorized access, alteration, disclosure or destruction; or any other risks to the security, confidentially or integrity of the information. Only authorized individuals with an identified purpose may have access to personal information.

5. Special Categories of Personal Information.

Personal information revealing racial or ethnic origins, political opinions or religious or philosophical beliefs, or trade union membership, as well as personal information concerning health or sexual life or other categories defined under domestic law may not be processed unless domestic law provides appropriate safeguards.

6. Accountability.

Public entities processing personal information [shall/should] be accountable for complying with domestic law and rules and on the protection of personal information.

7. Independent and Effective Oversight.

A system of independent and effective data protection supervision [shall/should] exist in the form of a public supervisory authority with effective powers of intervention and enforcement. These responsibilities may be carried out by a specialized public data protection authority or by more than one supervisory public authority to meet the particular circumstances of different legal systems.

8. Individual Access and Rectification.

[An/every] individual [should/shall] be provided with access to and the means to seek rectification and/or expungement of his or her personal information. In appropriate cases, an individual may object to processing of personal information related to him or her.

9. Transparency and Notice.

An individual [should/shall] be informed, as required by law, with general and individual notice at least as to the purpose of processing of personal information concerning him or her and who will be processing that information, under what rules or laws, the types of third parties to whom information is disclosed as well as other information insofar as is necessary to ensure fairness including rights and remedies available to the individual.

10. Redress.

[An/every] individual [shall/should] have an effective administrative remedy before a competent authority, [*and a remedy before an independent and impartial tribunal*] where his or her privacy has been infringed or data protection rules have been violated with respect to that individual. Any such infringement or violation [should/shall] be subject to appropriate and effective sanctions and/or remedies, such as rectification, expungement, or compensation.

11. Automated Individual Decisions.

Decisions producing significant adverse actions concerning the relevant interests of the individual may not be based solely on the automated processing of personal information without human involvement unless provided for by domestic law and with appropriate safeguards in place, including the possibility to obtain human intervention.

12. Restrictions on onward transfers to third countries.

Where personal information is transmitted or made available by a competent authority of the sending country or by private parties in accordance with the domestic law of the sending country to a competent authority of the receiving country, the competent authority of the receiving country may only authorise or carry out an onward transfer of this information to a competent authority of a third country if permitted under its domestic law and in accordance with existing applicable international agreements and international arrangements between the sending and receiving country. In the absence of such international agreements and international arrangements, such transfers should moreover support legitimate public interests consisting of: national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences, breaches of ethics of regulated professions, or the protection of the data subject. In all cases transfers should be fully consistent with these common principles, especially the limitation/purpose specification.

PENDING FURTHER DISCUSSION

The following five issues were identified High Level Contact Group as requiring equivalent attention as they relate to information sharing, privacy, and personal data protection in the area of transatlantic law enforcement cooperation. While text was proposed for most of these issues, no agreed upon language has yet been identified. The HLCG recommends that specific provisions detailing these issues be included in the negotiations toward the final product that will result from the HLCG's work:

13. **Consistency in private entities' obligations during data transfers;**
14. **Equivalent and reciprocal application of data privacy law;**
15. **Preventing undue impact on relations with third countries;**
16. **Specific agreements regulating information exchanges and privacy and personal data protection; and**
17. **Issues related to the institutional framework of the EU and US.**