EUROPEAN PARLIAMENT

Committee on Civil Liberties, Justice and Home Affairs [LIBE]

HEARING

Data Protection in a Transatlantic Perspective

Future EU-US data protection agreement in the framework of police and judicial cooperation in criminal matters

Monday 25 October, 15.00 – 18.30

Brussels
Room: ASP 3 E 002

Presentation
by

Douwe Korff
Professor of International Law

London Metropolitan University

London (UK)

Calcutta House
Old Castle Street
London E1 7NT, United Kingdom
d.korff@londonmet.ac.uk

European Parliament LIBE Hearing 25 October 2010:

Data Protection in a Transatlantic Perspective

Presentation by Douwe Korff

European Parliament LIBE Hearing 25 October 2010:
Data Protection in a Transatlantic Perspective
Presentation by Douwe Korff

Summary of points raised:

I. GENERAL CONTEXT AND TRENDS:

- Conflation of ideological struggle, war and and law enforcement;
- Bringing forward of the "battleground" (Cobler 1970s: *der vorverlegter Staatsschutz*);
- New technical capabilities (ubiquitous data generation, –capturing and –dissemination; data mining, analysis and "profiling") [but note the limitations!];
- Globalisation.

II. BASIC EUROPEAN AND CONSTITUTIONAL REQUIREMENTS:

- In Europe generally, and the EU specifically, data protection is a **fundamental right**, protected by the ECHR, general principles of Union law, the Charter of Fundamental Rights, and many national constitutions. *This is non-negotiable.*

- The **data protection principles and –criteria** in Articles 6 and 7 of the main EC DP Directive (95/46/EC) are specific expression**s** of general ECHR/Charter/constitutional requirements such as "law", "legitimate aim" (cf. purpose-limitation!), "necessity" and "proportionality" (cf. data quality requirements). **Data subject rights** are specific expressions of the ECHR requirement of an "effective remedy". Specifically, any "binding international agreement" on data transfers between the EU and the USA should:

  - meet the **"quality" requirements of "law"** specified by the EurCtHR and must thus be clear, precise, and foreseeable in its application, and provide protection against arbitrariness; and it must be fully published: wholly or partially secret rules can never constitute "law": the days of *Echelon*-type arrangements are over;

  - clearly relate the interferences with privacy it authorises to specific, **narrowly-defined purposes**. Prevention against immediate dangers, investigating and prosecuting criminal offences, and general intelligence are different purposes. Collecting and storing personal data "just in case" they may be useful to some purpose in the future is contrary to data protection law and Art. 8 ECHR.

  - clearly limit the data exchanges, and any further processing (including data retention), to what is **"necessary in a democratic society"** and **proportionate** to the specific purposes for which they took place (cf. the German Constitutional Court);

  - provide for **transparency** (informing of data subjects) and **effective remedies** and redress, including judicial redress: paper assurances are not adequate to protect fundamental rights (cf. the EurCtHR *re* assurance about torture).

- Any "binding international agreement" on data transfers between the EU and the USA that falls short of these requirements can be (and deserves to be) succesfully challenged; this would undermine the entire EU legal structure (**remember *Solange*!**).

III. THE DEFECTS IN THE CURRENT BILATERAL (MEMBER STATE – USA) AND PROPOSED NEW EU – USA ARRANGEMENTS IN THE ABOVE TERMS:

- The (full) details of the arrangements are often not made public; there is certainly insufficient transparency about them. This undermines democratic (in particular, parliamentary) accountability and control (at European and MS level);

- The arrangements use vague, catch-all clauses, the application of which are not foreseeable; they will lead to arbitrariness and indeed discrimination - it is highly doubtful whether they constitute "law" in the European-legal sense;

- The purposes of the data exchanges (in particular: export to the USA) are not clearly defined: different purposes are confused, as are the criteria for making data available:

> Example: Under the Germany – USA agreement, data may be made available to the USA if there are "clear and objective indications" (a criminal-law test) that the data subject is "involved" in "the terrorist environment". The seeming strictness of the first test is utterly undermined by the complete indeterminateness of the second and third tests.

- No clear justification or even rules are provided on what data can be disclosed for what purpose; rather, if there is a basic "hit", the floodgates [largely] open and [almost] everything is released (or at least can be released), including highly sensitive data which are certain to be irrelevant (e.g., sexual orientation) or likely to lead to discrimination;

- There are manifestly insufficient restrictions* on (i) the specific purpose for which specific data may be used; (ii) the specific bodies within the USA to which the data may be further disseminated (Note the restriction of the US statement on the extension of the principles in the Privacy Act to "DHS components"); and (iii) the retention of the data;

  * The term "manifestly insufficient restrictions" includes the inclusion, in various agreements or draft agreements, of unjustifiably opaque exceptions, exemptions and blatant loopholes. Agreements with such defects simply cannot be relied upon to perform as they suggest they will on their face, at first reading, especially in the absence of strict supervision.

- There are no restrictions on the use of data from the EU (EU bodies or MSs) for pernicious and dangerous "profiling" purposes in the USA;

- It is virtually impossible to provide tamper-proof technical measures to ensure compliance with such limited restrictions of the above kind as are provided;

- There is no real, effective review and oversight by European bodies or officials of compliance on the part of the US bodies that receive data from Europe;

- Individuals whose data have been disclosed to the USA have no effective (or effectively accessible) judicial or other remedies available to them in the USA; they should not be made to rely on vague assurances from the US authorities, or on possible support from European DPAs (who sometimes provide ineffective assistance even domestically). In any case, they will often be in the dark about the fact that their data have been disclosed in this way and/or how they are used (which in itself violates basic data protection principles).

IV. SUGGESTIONS FOR PROGRESS:

The basics:

- For "Europe" and the EU in particular, data protection is a non-negotiable fundamental right that must be respected and guaranteed, also in any EU – US data sharing arrangements. The EU legally cannot and in any case should not be willing (or feel compelled) to abandon this principle. If it did, it would undermine its own foundations.

- The USA too is a major democracy and knows about the rule of law. It has an enviably strong Constitution. It is capable of adopting and applying effective, enforceable safeguards for individuals, also in the areas of counter-terrorism and the fight against organised crime. See, for instance, the substantive limitations and important procedural safeguards adopted in respect of the interception of communications after Watergate and the Church Committee. Many of these were better than the corresponding substantive and procedural safeguards in European States, even now (except that they were limited to US citizens and permanent residents in the USA; and that President Bush ordered his officials to ignore them after 9/11).

- In a way, all we need is for the USA to accept the need for these kinds of safeguards, also in relation to the fight against terrorism and organised crime. Comprehensive protection of this kind must cover: (i) all US agencies and all databases and processing operations involved (rather than just "DHS components") and (ii) all data, on both US- and non-US citizens [at least when the data come from theEU]. It must also be enshrined in US law: **an international agreement, binding or not, cannot in itself guarantee the rights of those affected if the latter cannot invoke its supposed guarantees in the US courts.**

More specifically:

- The above would require *US laws domestically implementing the guarantees laid down in the agreement*. Both the international agreement and such laws should be:

  - fully transparent and open, rather than secret or semi-secret;

  - applicable to all anti-terrorism/organised crime data collecting and –use (including "profiling"), by all and any US body (and indeed by any private body contracted to carry out such activities) [at least when this involves data provided by the EU];

  - extended to "everyone" on whom the USA holds and processes data (whether they are US citizens or not) [or at least to all on whom the EU provided data];

  - "adequate" in the sense used in Directive 95/46/EC (and assessed to verify that);

  - subject to truly independent and impartial supervision and control by joint EU – US supervisory bodies with really effective powers of access, review and intervention;

  - fully justiciable in the US courts, again also by non-US citizens.

In my opinion, if the USA were to be willing to subscribe to the above in principle, and implement the above in its own domestic law, an agreement can be reached. If it were not to be so willing, no general agreement should even be considered.

European Parliament LIBE Hearing 25 October 2010:
Data Protection in a Transatlantic Perspective
Presentation by Douwe Korff

Structure:

- A multi-layered approach (as suggested by the EDPS) is indeed advisable. This would consist of a framework instrument setting out the basic principles and arrangements, supplemented by more specific instruments dealing with specific data exchanges for specific (narrowly-defined) purposes. The basic instrument should emphasise that the more specific instruments are subsidiary to the basic instrument.

- The basic instrument should contain express recognition by the EU and the USA of data protection/information privacy as a fundamental-right, and spell out the basic data protection principles, criteria, etc., to be followed. All the rest must be built on that; if that is not recognised the whole system is built on sand and will collapse.

- The basic instrument should require the Parties to implement the agreement, and any subsidiary or supplementary agreements, fully in their domestic law, in a way that ensures any individuals affected (of whatever country or nationality) access to the courts of the Party in question in respect of any action that affects them. Given that the data exchanges constitute "interferences" with a fundamental right, this is a basic requirement of the rule of law, and of the ECHR.

- The basic instrument should stipulate that, insofar as MSs can continue to enter into bilateral agreements on data sharing in this area with the USA, such Member State – USA agreements shall be compatible with the basic instrument, and shall in particular fully respect the human rights requirements under the EU Charter of Fundamental Rights and the ECHR. The basic instrument should commit the MSs to a review of their existing arrangements to that effect. (See also below, under the next sub-heading.)

- The basic instrument should also set out general supervisory arrangements, including close and real and effective oversight of what really happens by EU and US officials (as far as the EU is concerned, by the DPAs or the Commission acting with the WP29). The arrangements must ensure real and full access to all data and all databases of all the entities concerned. An appendix could spell out technical measures that should be taken to ensure that tamper-free logs etc. are kept and that supervision cannot be evaded.

- There should be comprehensive annual reports on the operation of the arrangements by the supervisory bodies, on both sides of the Atlantic.

- Before coming into effect, the basic instrument and each EU-generated specific instrument should be subject to an "adequacy" assessment by the Commission, working with the WP29, on the lines of the assessments of third country laws (and the US "Safe Harbor" agreement) carried out by the WP29 under EC Directive 95/46/EC. The assessment by the Commission and the views of the WP29 should be made available in full to the European Parliament in advance of its consideration of any draft agreement, together with the views of the EDPS.

Effect on existing Member States – USA and EU – USA agreements:

- All Member States – USA and all EU – USA agreements must, in theory, already comply with the ECHR and the relevant national constitutions. In reality, it seems clear that many do not do so: it is likely that some Member States – USA agreements at least will be succesfully challenged in the relevant domestic (constitutional) courts, and/or in the EurCtHR. EU – USA agreements are similarly subject to challenges in the ECJ and the EurCtHR - and indeed in domestic constitutional courts (*Solange* again!).

- The Commission should seek comprehensive information,including the full texts, of all existing arrangements between MSs and the USA in this field, and report to the Council and to Parliament on them, with full disclosure of the texts. The report should include a (non-judicial) assessment of the compatibility of these arrangements with the basic agreement, the Charter of Fundamental Rights, the ECHR, and the EU *acquis* in the field of data protection. The EU can, in my opinion, take such interest because these arrangements impact on EU-internal and –external arrangements: if some MSs pass on data to the USA, that could affect the operation of intra-EU data flows; and the EU – USA agreements too should take account of the existing Member States – USA agreements.

- In my opinion, even following the adoption of a basic EU- USA agreement, and indeed some more specific EU – USA agreements, existing Member State – USA agreements can continue to have effect as long as the particular matter has not (yet) been covered by a specific EU – USA agreement - but subject to the stipulation mentioned earlier, that they be reviewed for their compatibility with the basic agreement and with the Charter of Fundamental Rights and the ECHR.

- However, whenever a specific EU – USA agreement is adopted, it shall (after a suitable implementation/transition period) override previous EU – USA and exisiting Member State – USA agreements on the same matter. Given the complexity of the issues (including the question of what constitutes a "same matter"), a report should be drawn up to accompany each proposed new specific EU – USA agreement, that lists the relevant Member State – USA agreements that will be affected (and possibly terminated) by the new specific EU – USA agreement.

- o – O – o -

Douwe Korff
Cambridge/London, 24 October 2010

To follow: Selected extracts / References