EUROPEAN COMMISSION – DG JFS

NEW CHALLENGES TO DATA PROTECTION

FINAL REPORT

Executive Summary

I. Aim of the Study

The purpose of the study was to identify the challenges for the protection of personal data produced by current social and technical phenomena such as the Internet, globalisation, the increasing ubiquity of personal data and personal data collection, the increasing power and capacity of computers and other data-processing devices, special new technologies such as RFID, biometrics, face-recognition, increased surveillance (and "dataveillance"); and increased uses of personal data for purposes for which they were not originally collected, in particular in relation to national security and the fight against organised crime and terrorism; and to produce a report containing a comparative analysis of the responses that different regulatory and non-regulatory systems (within the EU and outside it) offer to those challenges, and that provides guidance on whether the legal framework of the main EC Directive on data protection (Directive 95/46/EC) still provides appropriate protection or whether amendments should be considered in the light of best solutions identified.

The study covered the following countries and jurisdictions: the Czech Republic, Denmark, France, Germany, Greece and the UK; and outside Europe, the USA (Federal level, California and New Jersey), Australia, Hong Kong, India and Japan.

II. The Challenges

The plunging cost of storing, transmitting and processing personal data means that little technological or economic incentive remains for system designers to minimise the collection of such data. "Web 2.0" technologies allow users to share (often sensitive) information about themselves and those around them to an unprecedented degree. Remotely-readable RFID tags are now often attached to consumer goods, while similar tags are included in many nations' passports and are also being used for road toll payment systems, public transport ticketing, library book management, and in new contactless payment cards such as MasterCard's "PayPass" and Visa's "Paywave". CCTV cameras are proliferating in urban areas and on roads, with automatic recognition of car number plates. Biometrics such as facial images and iris scans are increasingly used to identify individuals. All such information can moreover be transferred around the world at low cost, and duplicated across databases and portable computing devices. Anonymisation of data will be increasingly impossible to achieve. These technological developments will produce a "digital tsunami" of data about individuals, which are accessible for surveillance and marketing purposes, and can be used to exercise control over the individuals.

Ongoing increases in processing power allow more information to be extracted from this mass of data, using data mining algorithms to discern patterns of behaviour and create "profiles" that in turn affect how individuals are treated. Public concerns over terrorism have led governments to share and analyse data about individuals' travel, finances and communications. E-government systems, intended to improve public service provision while reducing overall costs, are often built around population-scale databases containing sensitive personal data on millions of citizens. These records are commonly interconnected, analysed and "mined" to achieve state goals, at the expense of democratic and data subject control. Increasingly, "the computer" takes decisions that "significantly affect" individuals, on the basis of dynamically-created algorithms that even the officials or staff implementing the decisions do not understand, and that data subjects are unable to challenge. Data protection is

not (just) about privacy: it is about countering these increasing threats to fundamental European values.

Effective data protection therefore now depends upon the robust application of principles such as purpose limitation and the minimisation of personal data collection during the design phase of information system engineering; and careful scrutiny of the proportionality of government and private-sector databases and surveillance programmes.

III/IV. Fundamental Imperatives and Basic Approach

Any review of the EU data protection regime should start with explicit recognition of the need to meet the requirements of the ECHR and the Charter of Fundamental Rights, and of the constitutions of the Member States. Failure to do so will endanger core European constitutional values and violate general principles of EU law, and will threaten the acceptance of the supremacy (or primacy) of EC and EU law by the constitutional courts of several Member States. More specifically, the basic European data protection principles, rules and criteria are part of that fundamental human rights fabric, and have stood the test of time, even if they may need strengthening in some respects.

However, their specific application and enforcement has been much less successful, and the new technological developments threaten to make the application of the principles yet more difficult (although some new technologies can help in their application).

Data protection law in the EU (in all areas covered by the previous three pillars) can and should therefore continue to rest on the basic data protection principles and criteria set out in Directive 95/46/EC. The application of these broad standards needs to be clarified, but they themselves do not require major revision in order to meet the new challenges. On the contrary, they reflect European and national constitutional/human rights standards that need to be strongly re-affirmed.

V. Recommendations (only)

The study identified the following issues as those which any review of the EU data protection regime should focus, and formulated the following recommendations on those issues (References in brackets are to the sections in Part V of the Final Report where these matters are discussed in detail):

- ✓ **The problematic exclusions of certain matters from the scope of the Directive** (V.2):

(i) Former First and Third Pillar matters:

Recommendation: The basic data protection principles, rules and criteria enshrined in the Directive must be applied "seamlessly" to activities in all the areas previously covered by the different pillars. This includes the application of the (limited) exceptions for the old third-pillar activities listed in Article 13 of the Directive. If the challenges are to be met, there will have to be greater harmonisation, or at least approximation, of data protection rules covering those activities in the EU, based on COE Recommendation R(87)15. Also crucial is full judicial protection in the national courts, and through the ECJ with data subjects having full standing (with the back-stop being the European Court of Human Rights).

(i) Exceptions for purely personal processing and freedom of expression, in particular in relation to social networking sites and "blogging" on "Web 2.0":

Recommendation: It should be possible to apply data protection rules more lightly to relatively trivial activities on the Internet. We believe that the best way to address this problem is to regulate services that ordinary users rely on, particularly social networking sites. Companies should be made to provide default settings for their sites and services and tools that are privacy-friendly: if the default settings fail to protect privacy and personal data, the site that chose those settings should carry the primary responsibility for this. This would leave open the possibility of adopting (or where they already exist, retaining) a tort [civil wrong or *faut*] regime under which individuals can be held liable for wrongful or unjustified public disclosure of private information or "intrusion" over the Internet.

✓ **The vexed question of "applicable law"** (V.3)

Recommendation: Better, clearer and unambiguous rules are desperately needed on applicable law. We would tentatively suggest rules on the following lines (see the full Final Report for *caveats* to these suggestions):

– *within the EU/EEA*, the rules should, in our opinion, simply be based on the "country of origin" principle, as originally intended. However, it is an essential prerequisite for this that there is greater harmonisation, or at least approximation at a high level, between the laws of the Member States (see below).

– *non-EU/EEA companies "established" in the EU/EEA* should be able to comply only with the law of their EU/EEA country of main establishment (their European HQ), and should otherwise be treated as EU/EEA companies.

– in relation to *non-EU/EEA companies not "established" in the EU/EEA but that use "means" in the EU/EEA* (typically, non-EU/EEA companies that offer products or services to EU/EEA citizens and companies over the Internet), the rules on "applicable law" should be simplified, so that they too can adhere to the law in one (relevant) EU/EEA country only. Consideration could be given to making this choice of law possible within such a company's Binding Corporate Rules; the appropriateness of the choice of law would be one of the issues to be assessed in judging the adequacy and appropriateness of the BCRs.

– *non-EU/EEA companies that are subject to an "adequate" law* in their country (as determined by the Commission) should be treated on a par with EU/EEA companies, i.e., they should only have to comply with their own ("adequate") law - provided the States concerned also comply with the measures taken in the EU/EEA to ensure ongoing harmonised/approximated application of the law.

✓ **The need for much greater harmonisation (at a high level) within the EU/EEA, through various means including stronger enforcement action by the Commission** (V.4)

Note: The study examined in some detail the differences in the laws of the Member States on important issues such as: **core concepts and definitions** (V.4.A(i)), the **data protection principles** (V.4.A(ii)) and –**criteria** (V.4.A(iii)); processing of **sensitive data** (V.4.A(iv)); the rules on **transborder data flows** (V.4.A(v)); and the **laws of non-EU/EEA States** in these respects (V.4.B). The findings are in Part V, section 4; the full details in Working Paper No. 2. The basic conclusion is that there remain major differences in all these respects.

Recommendations: We do not recommend that the Directive should be replaced by a Regulation or a new, more tightly-drafted Directive. Rather, we recommend that the WP29 be asked, in consultation with the Commission (which in any case serves as its Secretariat) to carry out more, and more in-depth, surveys of national law and practice, with a view to formulating "best practice" and suggested interpretations (which is basically what they do already), but with an added requirement that the Member States should report on the extent to which they comply (or feel they should not have to comply) with such suggestions. It would then be up to the Commission, if needs be, to test out whether the WP29 guidance is the one that, in law, should be followed by the Member States - with enforcement action being considered as a normal means of testing this if required. We believe that this would not require any amendment to the Directive. However, it would signal a major difference in the Commission approach to ensuring more harmonised transposition and implementation of the directives, with WP29 opinions effectively, in appropriate cases, enforced by the Commission (subject, of course, to the supervision of the ECJ).

As a very modest step in that direction, aimed at enabling such actions by both the WP29 and the Commission, we recommend that, at least, the views of the WP29, and the extent and manner in which they are reflected in national law and practice in the Member States, be made available in a more structured, comprehensive form, and that the attention of relevant administrative and judicial bodies at national and EU level be drawn to them.

- ✓ **The need for more cooperation with non-EU countries, and greater recognition of "adequate" non-EU efforts** (V.5)

Recommendation: The "adequacy" process has not (yet?) had the impact that it potentially could have and should be reviewed. Perhaps provisional rulings could be an answer. In any case, the other, less formal measures, such as technical assistance, close cooperation (including "twinning" of EU and non-EU DPAs), and other processes should continue and be strongly supported. In the meantime, it is important, at a political level, to reverse the process of Article 25 of the Directive losing its potential international impact.

- ✓ **the need to ensure much greater compliance with and much stronger enforcement of existing law, at the domestic level, by the DPAs** (V.6)

Recommendations: We recommend that there should be "prior checking" of population-scale information systems in the Member State, especially in the public sector - but (i) before they are cast in concrete (i.e., starting in the early planning stage) and (ii) by better (technically) qualified staff. It is notable that the Australian Government has recently proposed that the Privacy Commissioner in that country should be given the power to require government agencies to prepare Privacy Impact Assessments. In the private sector, a similar role could be fulfilled by Privacy Audits or (real and effective) Privacy Seals, strongly encouraged by public procurement rules giving competitive advantage to data protection-compliant products and services (as is already the case in Schleswig-Holstein in Germany) (see below). More generally, we feel that consideration could be given to moving enforcement largely away from the DPAs, to the courts and the prosecuting authorities.

- ✓ **The need to strengthen the rights and remedies for individuals (possibly acting with or through relevant NGOs)** (V.7)

Recommendations: The basic requirements that should be met in order to make the "judicial remedy" referred to in Article 22 truly effective should be discussed in the WP29, and guidance issued in this respect - and the Commission should take enforcement action if

these requirements are not met. A study should be commissioned to look into possible means of supporting individuals in this respect, e.g., by changing rules on litigation costs; by allowing non-governmental/civil society groups to support, or be formally involved in, proceedings by individuals, or to act on behalf of groups of data subjects; by providing for default, liquidated damages awards; or by adopting special systems such as the US "*qui tam*" procedure.

- ✓ **the need to further develop supplementary and alternative measures (while understanding the built-in limitations and practical restrictions of such measures)** (V.8)

Note: The study examined in some detail both the potential benefits and the limitations - and the often deceptive, or broken, promises - of **Privacy Enhancing Technologies (PETs)**, including encryption (as a means of ensuring compliance with at least data security requirements) and a related issue: security breach notification; de-identification; and others, such as P3P and online subject access systems; **Privacy-Friendly Identity Management**, including (now largely outdated) centralised systems, more recent "user-centric" ones, "vendor relationship management systems", and the use of identity cards for miscellaneous purposes; **Privacy by Design**, including the use of Privacy Impact Assessments; **User Privacy Controls and Default Settings**; **Sectoral Self and Co-Regulation**; and **Privacy Seals**. Here, it must suffice to note our overall conclusions.

Recommendation: Any view of complementary and alternative measures must be based on realistic and technically correct evaluations of such measures. They should not be dismissed out of hand. However, they will have to be closely scrutinised, by technical as well as legal experts.

It may be useful to consider the establishment of a special body or office of the EU/EEA DPAs, closely linked to the WP29 and the Commission, to deal with the European Privacy Seal, European codes of conduct, and Binding Corporate Rules, on a quasi-commercial (or at least fully self-financing) basis, in a way similar to the system in Schleswig-Holstein.

Overall, the question of incentives and economics of privacy and data security are central. If the law makes the protection of privacy economically attractive (e.g., through procurement incentives, coupled with the issuing of serious privacy seals), or punishes breaches of data protection and data security rules (by placing the onus for protection on those who are in the best position to ensure them, rather than by allowing them to shift the costs to others, such as consumers), then data protection can have a future. We believe that requires the right combination of law and self or co-regulatory rules and mechanisms. We hope the above gives some food for thought on these.

- o – O – o -

Core experts:
Prof. Douwe Korff (UK/Netherlands)
Dr. Ian Brown (UK)

Special experts:
Prof. Peter Blume (Denmark)
Prof. Graham Greenleaf (Australia)
Prof. Chris Hoofnagle (USA)
Prof. Lilian Mitrou (Greece)
Filip Pospíšil, Helena Svatošová,
& Marek Tichy (Czech Republic)

Advisors:
Prof. Ross Anderson (UK)
Caspar Bowden (UK/France)
Prof. Katrin Nyman-Metcalf (Estonia)
Paul Whitehouse (UK)