US Safe Harbour Principles Come Under Fire

ON MARCH 8TH 2001, the US Subcommittee on Commerce, Trade, and Consumer Protection heard several witnesses on the implications of the EU Data Protection Directive for US privacy policies.

Among the witnesses were Professor Stefano Rodota, Italy's Data Protection Commissioner and Chairman of the EU Data Protection Working Party, David Smith, Assistant Commissioner, Office of the UK Information Commissioner, and Professor Joel Reidenberg, Professor of Law, Fordham University School of Law, New York.

David Smith submitted evidence on behalf of the UK Information Commissioner. He outlined the origins of data protection in Europe, EU Data Protection Directives and the UK Data Protection Act 1998. He also explained what is meant by an "adequate level of protection" when dealing with transfers of personal data abroad, Community findings and exceptions to the requirement for adequacy, including the role of standard contracts.

Professor Stefano Rodota spoke of the US Safe Harbour (SH) principles as "living proof that the Directive allows significant flexibility". He stated that, in finding that the SH offers adequate protection, the European Commission may have gone beyond the letter of Article 25, which refers to "domestic law" or international commitments, and has accepted a set of rules that are proposed to US companies on a voluntary basis. However, he did not want to reopen that debate. He merely stressed that on the European side there had been "a lot" of good will. He also expressed concern that only 25 US organisations had adhered to the Safe Harbour up to that point.

Professor Joel Reidenberg noted that the European Directive exerts significant pressure on US information rights, practices and policies. The Directive forces scrutiny of US data privacy. "In this context, the lack of legal protection for privacy in the United States threatens the flow of personal information from Europe to the United States. At the same time, the EU Directive is having an important influence on privacy protection around the world and leaves Americans with legal protections as second class citizens in the global marketplace."

Among the specific flaws of the Safe Harbour, Professor Reidenberg identified the following:

• Both national supervisory authorities and the European Commission must assess the level of protection offered in the United States to data of European origin. Because the United States lacks directly comparable, comprehensive data protection legislation, the assessment of "adequacy" is necessarily complex.

• With a high level of legal protection available on a cross-sectoral basis, Europeans do not face the same privacy obstacles for e-commerce that currently threaten American business. The culture of legal protection in Europe provides European companies with a competitive privacy advantage doing business in Europe over the many American companies that are unaccustomed to applying fair information practices to personal information.

The end result for American companies was that "US corporate information practices are under scrutiny in Europe and under threat of disruption when fair information processing standards are not applied to protect European data." Professor Reidenberg noted that some commentators have predicted that any European export prohibition might spark a trade war that Europe could lose if brought to the new World Trade Organisation. He considered an adverse WTO ruling unlikely.

• U.S. companies recognize that they will have to respect European legal mandates. Unless American companies doing business in Europe chose to flout European law, US multinational businesses must provide stringent privacy protections to data of European origin when processing that data in Europe or in the United States.

American law and practice allow those same companies to provide far less protection, if any, to data about American citizens. American companies will either provide Europeans with better protection than they provide to Americans or they will treat Americans in accordance with the higher foreign standards and disadvantage those citizens doing business with local US companies.

• While the approval of the Safe Harbour was an important short-term political victory for both the US and the European Commission, the SH agreement is unworkable for both sides and will not alleviate the issues of weak American privacy protection. Professor Reidenberg argued that the

SH offered a mechanism to delay facing tough decisions about international privacy. He argued that it became a mechanism to avoid a showdown judgment on the status of American law and defer action against any American companies. He called the acceptance in July 2000 of the Safe Harbour by the European Union a "transitory political success."

• The dubious legality of Safe Harbour. The underlying legal authority of the Federal Trade Commission (FTC) to enforce the SH is questionable.

• Within Europe, the legality of SH is also open to question. Under the European Directive, "adequacy" must be assessed in light of the prevailing "rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country." However, the Safe Harbour was not yet in existence at the time of the approval by the European Commission.

The European Parliament specifically noted this problem shortly before the approval by the European Commission. Similarly, according to the European Directive, the European Commission only has authority to enter into negotiations to remedy the absence of "adequate" protection after a formal finding that the non-European country fails to provide "adequate" protection. Yet, in the context of the SH negotiations, the European Commission never made a formal finding. These would appear to be significant administrative law defects.

This administrative process problem remains an open question that only the European Court of Justice can resolve and gives the independent national supervisory authorities grounds to vitiate Safe Harbour through strict interpretations of the European Commission's ruling.

• Violation of Treaty Establishing the EC: The European Parliament pointed out the risk that the exchange of letters between the Commission and the US Department of Commerce on the implementation of the SH principles could be interpreted by the European and/or United States judicial authorities as having the substance of an international agreement adopted in breach of the Treaty establishing the European Community and the requirement to seek Parliament's assent.

• Limited Applicability: The scope of the Safe Harbour is very narrow. First, by its own terms SH can only apply to activities and US organisations that fall within the regulatory jurisdiction of the FTC and the Department of Transportation. As a result, many companies and sectors will be ineligible for Safe Harbour

including particularly the banking, telecommunications and employment sectors. These latter organisations are expressly excluded from the FTC's jurisdiction. Second, the Safe Harbour will not apply to most organisations collecting data directly in Europe.

• Increased Risk to Non-Safe Harbour Transfers: By implication, the Safe Harbour raises the risks for data transfers by companies that do not subscribe to the code. The approval by the European Commission of Safe Harbour as an "adequate" basis to transfer personal information to the United States implicitly acknowledges that transfers outside the scope of the SH will not be adequately protected. Consequently, non-SH transfers must be covered by one of the other exceptions to the transborder data flow rules, such as a transfer pursuant to a contractual arrangement.

• For the United States, the SH approach might compromise many US businesses in a way that a legislative solution would not: Safe Harbour simplifies the task for national supervisory authorities to block data flows to the US. The national agencies will readily be able to identify those US companies that do not subscribe to SH and have not presented a data protection contract for approval under the European Directive's Article 26 exceptions. In such cases, the presumption must be that the protection is "inadequate" and the data flow must, under European law, be prohibited.

• Weakening of European Standards and Illusory Enforcement Mechanisms: For the national supervisory authorities in Europe, the Safe Harbour poses a weakening of European standards. In particular, the permissible derogations from SH without a loss of coverage are significant. Most important, SH weakens European standards for redress of data privacy violations. Under the European Directive, victims must be able to seek legal recourse and have a damage remedy. The Department of Commerce assured the European Commission that Safe Harbour and the US legal system provided remedies for individual European victims of SH violations. The EC expressly relied on representations made by the Department of Commerce concerning available damages in American law. The memorandum presented by the Department of Commerce to the EC, however, made misleading statements about US law.

• The enforcement provisions of the Safe Harbour rely on the FTC: Even if the FTC has jurisdiction to enforce the SH, the assertion that the FTC will give priority to European enforcement actions is hard to believe. First, although the FTC has become active in privacy issues recently, the agency's record enforcing the Fair Credit Reporting Act, one of the country's most important fair information practices statutes, is less than aggressive. Second, were the FTC to devote its limited resources to the protection of Europeans' privacy, Americans should and will be offended that a US government agency charged with protecting American consumers has chosen to commit its energies and US taxpayer money to the protection of European privacy in the United States against US businesses at a higher level than the FTC asserts for the protection of Americans' privacy.

Professor Reidenberg testified that the consequence of these standards, the unenthusiastic reception of the Safe Harbour and enforcement weaknesses is a likelihood that the national supervisory agencies will be dissatisfied with the Safe Harbour and that the Member States will eventually face great political pressure to suspend the Safe Harbour.

The full list of witnesses and the complete transcripts of their testimony before the subcommittee can be found at: http://www.house.gov/commerce/hearings/03082001-49/03082001.htm

Continued from page 7

not prosecuted or is acquitted of the offence, the sample must be destroyed and the information derived from it cannot be used.

The subsequent decision of the House of Lords overturned the ruling of the Court of Appeal.

The House of Lords ruled that where a DNA sample should have been destroyed, but had not been, although section 64 of PACE prohibited its use in the investigation of any other offence, it did not make evidence obtained as a failure to comply with that prohibition inadmissible. It was left to the discretion of the trial judge. The Bill removes the requirement of destruction, and provides that fingerprints and samples lawfully taken on suspicion of involvement in an offence or under the Terrorism Act can be used in the investigation of other offences. This new measure will bring the provisions of PACE for dealing with fingerprint and DNA evidence in line with other forms of evidence.

The Criminal Justice and Police Bill is on the website at http://www.homeoffice.gov.uk The Home Office proposals, published by the Home Office Communication Directorate, is also available from the same website.