

April 28, 2000



UPDATE ON SAFE HARBOR DISCUSSIONS

For almost three years, the U.S. and the European Commission have been in negotiations over the conditions under which companies in the U.S. can lawfully receive and process personal data from Europe. Final agreement on these terms may be reached this summer, and companies that handle information from Europe about customers, travelers, employees, job applicants, sales contacts, patients, and web site visitors should watch these developments closely.

BACKGROUND. Many American companies are already assessing their obligations under new U.S. federal privacy laws — such as Title V of the Gramm-Leach-Bliley Financial Modernization Act of 1999 (see February 2000 ECommerce News) and the Children’s Online Privacy Protection Act of 1998 (see October 1999 ECommerce News). (Note that COPPA went into effect on April 21 of this year.) The majority of the states also have privacy bills pending that are designed to extend the reach of the federal acts and cover additional consumer or employee privacy concerns.

At the same time, however, multinational companies will have to decide how they will comply with comprehensive national data privacy laws in Europe implementing the EU Data Protection Directive (Directive 95/46/EC).

Article 25 of the EU Directive forbids the transfer of personal data outside the EU to countries lacking

“adequate” levels of data protection. The U.S. has not been deemed to provide “adequate” protection of personal data privacy as a matter of law, because the U.S. has specific data privacy laws but nothing equivalent to the European approach of broadly regulating any commercial use of personal data.

SAFE HARBOR. The U.S. Department of Commerce and the European Commission have been locked in nearly three years of discussions concerning a voluntary set of “Safe Harbor” principles and procedures under which American companies could be allowed to handle European personal data in the U.S. In general, companies that agree to the Safe Harbor principles of notice, choice, and access must notify consumers of the purpose of data collection; allow consumers the opportunity to opt out of their data being shared with third parties; and provide users with access to their personal information.

The basic concept of Safe Harbor is that a company in the U.S. could certify to the Department of Commerce that it handles personal data from the EU consistently with the published Safe Harbor principles. The company would have to designate an independent third party capable of investigating the company’s compliance and sanctioning its non-compliance. That third party could be a U.S. regulatory body, where appropriate, or a self-regulatory regime such as BBBOnline, or even simply an agreement to

cooperate with a panel of European data protection authorities.

WHAT WILL BE THE IMPACT OF SAFE HARBOR? The Safe Harbor arrangements are likely to serve as a model not only for data flows between the U.S. and the 15 EU Member States, but also with other European countries whose data protection laws are similar to the EU Directive — and with the growing number of non-European jurisdictions (such as Hong Kong, Taiwan, New Zealand, and, soon, Canada and Australia) with broad personal data privacy laws and restrictions on foreign data transfers.

Moreover, the Safe Harbor principles include conditions for safely transferring EU data onward to an affiliate or business partner beyond the U.S. Thus, if the U.S. and EU agree on Safe Harbor, a standard may be set for global data flows, despite the many remaining differences in national laws and procedures.

WHAT IS THE STATUS OF SAFE HARBOR DISCUSSIONS? Last month, Brussels and Washington reached an agreement on the text of Safe Harbor principles and accompanying FAQs.

But the proposed Safe Harbor arrangements, which can be found on the Department of Commerce web site at www.ita.doc.gov/td/ecom/menu1.html, have not been finally approved on either side of the Atlantic.

The European Commission is required to seek opinions on the Safe Harbor proposal from the European Parliament and the “Article 29 Working Group” representing the independent data protection authorities of the EU Member States. Those opinions could be persuasive, but they do not bind the Commission.

However, the Commission’s proposal *can* be overturned by a weighted majority vote of the “Article 31 Committee” representing the Member State governments themselves. That group met March 30-31 and, somewhat surprisingly, declined to approve the Safe Harbor proposal. The Article 31 Committee asked the Commission to seek further assurances from the U.S. on effective enforcement. The Member States remain skeptical about self-enforcement schemes such as BBOnline and do not fully understand the role that

the FTC and states will play in enforcing corporate privacy commitments. The Article 31 Committee will meet again at the end of May. Unless they muster a weighted majority against the Commission’s proposal, it will go into effect as a binding EU measure.

ARE DATA FLOWS FROM THE EU TO THE U.S. LIKELY TO BE BLOCKED DURING THE NEXT MONTH? No. While the Safe Harbor talks have been going on, the European Commission has provided an “informal” undertaking from EU Member States not to block data flows to the United States (unless specific and serious abuses take place). American companies often refer to this as a “standstill agreement,” but in fact it is a tenuous political agreement rather than a treaty or legal obligation. The Member States have requested forbearance from their national data protection authorities (typically independent commissions somewhat analogous to the Federal Trade Commission in the U.S.). This does not, however, preclude an administrative investigation or a judicial action seeking injunctive relief or damages.

The European Commission has recommended the Safe Harbor arrangement as a means of assuring “adequate” protection of personal data received from Europe, and proposes maintaining the informal enforcement standstill until an implementation review is conducted in mid-2001.

WHAT ARE THE IMPLICATIONS FOR GLOBAL COMPANIES? There is a possibility of a final Safe Harbor agreement by June, but there is also the possibility of further modifications and delays, or even a breakdown in the process. The latter would raise the prospect of an end to the informal standstill and immediate pressure on multinationals to justify any data transfers by *consents*, *contract performance*, or approved *contractual safeguards* between the parties in the EU and the U.S. The Commission has promised to work on developing Europe-wide approved contract clauses for the latter method, but so far there are no models used routinely across Europe. Instead, companies using contractual safeguards for transborder data flows have had to comply with national laws and, often, seek formal or

informal opinions from national data protection authorities.

Companies handling personal data from the EU may choose to await the results of the Safe Harbor negotiations. They do take some risk in the event of a judicial action or a breakdown in the talks and, therefore, an end to the informal enforcement “standstill.” Companies may want to examine their data flows, especially if they are in the course of data processing consolidation projects or implementing intranets or enterprise software (such as SAP or PeopleSoft) that will result in more European data being accessible outside the EU.

MONTHLY UPDATE

CHINA PERMANENT NORMAL TRADE RELATIONS (PNTR). House Speaker Dennis Hastert announced that the House will vote on whether or not to extend normal trade relations status to China on a permanent basis. This year, in order to avoid the yearly battle over the matter and to smooth the path for China’s entry into the World Trade Organization, Congress will be voting to confer the trade status permanently. Senate Majority Leader Trent Lott has indicated a Senate vote would likely occur in June.

ELECTRONIC SIGNATURES. House and Senate conferees have not formally met to negotiate a compromise on legislation (H.R. 1714, Rep. Bliley and S. 761, Sen. Abraham) that would confer legal validity on electronic signatures. However, staff from both sides have met to discuss a proposal by Senate Commerce, Science, and Transportation Committee Chairman, John McCain (R-AZ); Commerce Subcommittee on Manufacturing and Competitiveness Chairman Spencer Abraham (R-MI); and Banking Chairman Phil Gramm (R-TX), to provide “more clarity and certainty to the bill,” in order to stave off legal challenges. House Commerce staff reportedly are not sold on the proposal, which they say is a significant departure from the House-passed version. Meanwhile, the technology industry is stepping up its efforts to educate Members of Congress on the significance of the bill and its effects on ecommerce as well as the financial services industry. Both chambers

passed their respective bills last November.

FASB. The Federal Accounting Standards Board (FASB) continued its endeavors to eliminate the “pooling method” of accounting, despite calls from Congress to slow down and consider the serious harm such an action could inflict on the economy. The independent board, which is seeking to ensure that accounting for business combinations provides investors with accurate information, voted against a proposal to expand the project which would have the effect of slowing down the process.

The House Commerce Subcommittee on Finance and Hazardous Materials has scheduled a hearing on the matter next month. At a similar hearing earlier this year before the Senate Banking Committee, technology industry representatives discussed the negative consequences that the elimination of pooling would have on technology industry mergers, the ability to attract capital, and the overall health of the economy.

INTERNET TAXATION. The Advisory Commission on Electronic Commerce has formally submitted its report to Congress, despite not having reached a supermajority consensus (as required by the law that created the commission). Virginia Governor James Gilmore, who chaired the commission, testified before the House Commerce Committee in support of the report. The report recommends that Congress repeal the three-percent excise tax on telephone services, permanently ban Internet access charges imposed by states and localities, and extend the current Internet tax moratorium on multiple and discriminatory taxation for an additional five years.

Legislation already has been introduced to implement some of the recommendations of the commission. Sen. John McCain (R-AZ), Chairman of the Senate Commerce, Science and Transportation Committee, introduced legislation (S. 2255) to extend the Internet tax moratorium until 2006. However, Chairman McCain postponed consideration of his bill because the outcome of a vote on the measure was uncertain.

Senators Herb Kohl (D-WI) and Judd Gregg (R-NH) have introduced legislation (S. 2401) to clarify the “nexus” issue. The legislation would relieve businesses with no physical presence in a state from collecting sales taxes in that state. Among the many examples of what does *not* constitute nexus, the bill includes “the use of an Internet service provider, on-line service provider, network communication service provider, or other Internet access service provider, or World Wide Web hosting services to maintain or take and process orders via a web page or site on a computer that is physically located in such State.”

INTERNET GAMBLING. The House Judiciary Committee passed The Internet Gambling Prohibition Act (H.R. 3125), sponsored by Rep. Bob Goodlatte (R-VA). The bill provides for up to four years’ imprisonment and a \$20,000 fine on conviction for operating an illegal Internet gambling site.

MP3 RULING. On April 28, a federal district court judge in New York said that MP3.com had violated record company copyright rights, and granted plaintiffs’ motion for partial summary judgment against MP3. MP3’s service allows customers to listen to CDs through the site, as long as the customer proves he or she already owns a copy of the CD in question. The Recording Industry Association of America claimed that MP3.com’s electronic database of

recordings (compiled without permission from rights holders) violated the copyrights of its members. RIAA will likely ask for an injunction against MP3.com within the next few days.

MICROSOFT REQUEST. On April 28, the Department of Justice and several state attorneys general asked Judge Thomas Penfield Jackson (D.D.C.) to divide Microsoft into two companies — one to sell Windows operating systems, and one to sell software applications.

PRIVACY SURVEY. In early April, Enonymous.com released a privacy survey ranking 30,000 sites based on their treatment of data. The survey said that of the 1,000 most-trafficked sites on the Web, only 8.6% deserved “four stars” for their privacy practices. But the survey appears to be full of factual errors and oversights. For example, the Electronic Privacy Information Center site, epic.org, received only two of a possible four stars from Enonymous, prompting EPIC to announce that “[Enonymous] doesn’t even have close to a clue about evaluating a privacy policy.”

For further information, contact:

Susan P. Crawford scrawford@wilmer.com
202/663-6479
Lynn R. Charytan lcharytan@wilmer.com
202/663-6455

This memorandum is for general purposes only and does not represent our legal advice as to any particular set of facts, nor does this memorandum represent any undertaking to keep recipients advised as to all relevant legal developments.

ECommerce News is a publication of WCP’s EGroup.