European Commission avoids privacy dispute with the USA

Professor Joel R Reidenberg, Fordham University School of Law, New York

AS A LEADING AUTHORITY on Safe Harbor, Professor Reidenberg considers the Commission's report has seriously understated the flaws in the scheme.

The European Commission's Staff Working Paper on the implementation of the US-EU Safe Harbor Agreement is striving to avoid a privacy dispute with the US in the aftermath of September 11th. Whilst September 11th has focused attention on government access to personal data, Safe Harbor addresses a different set of issues.

The agreement itself was an attempt to solve the obvious legal conflict between the principles in the European Directive and the lack of rules and standards in the US for the treatment of European personal data by US companies. The political hope was that Safe Harbor would create a substitute for missing US legal protections for European data. Because the European Parliament was critical of the acceptance of a prospective arrangement, the Commission committed to an assessment of the agreement's implementation.

This resulting paper tries to put a positive spin on the first 18 months of Safe Harbor, but clearly illustrates that compliance with the arrangement falls short of the expected level of data protection. The paper looks at the implementation by US companies of the Safe Harbor principles based on an independent consultant's study of "visible compliance" as of June 2001, and on information gathered by the Commission. The Commission also had responses from the US Department of Commerce.

On the positive side, the report emphasises that Safe Harbor simplifies data exports to the US, that few complaints have been filed thus far, and that various dispute resolution groups in the US might meet the requirements of the Safe Harbor. The report also praises the US Department of Commerce for its efforts to develop compliance workbooks for US companies and the Federal Trade Commission (FTC) for its responsiveness to the European Commission.

Nevertheless, the reported compliance deficiencies are significant. First, only a trivial number of US companies were participating in the Safe Harbor, and only a few of those were major corporations engaged in international data flows.

Second, the Staff Paper notes that "a substantial number" of participating companies have failed to provide the required transparency. This failure shows that corporate compliance with one of the most basic principles of the Safe Harbor is seriously lacking. US companies are not accustomed to publicly describing their data processing practices. The significant level of non-transparency suggests participants are trying to create an appearance of data protection and that they do not foresee any real consequences for deficiencies.

Third, and equally troubling, the paper observes that fewer than 50 per cent of the participating companies complied with all of the required Safe Harbor principles. While the report attributes some of the non-compliance to "teething problems", this extraordinary failure rate calls into question the very legitimacy of the current agreement as a substitute for missing legal protection.

Lastly, the validity of the entire Safe Harbor arrangement rests on the commitment by the FTC to bring enforcement actions against breaching participants. The Staff Paper notes an assertion by the FTC that the lack of transparency would be actionable as an "unfair and deceptive trade practice".

But, despite transparency failures and widespread omissions in privacy policies, the paper also shows that no company has been pursued for making a false self-certification to the US Department of Commerce. Indeed, there is no support in American law for the dubious assertion by the FTC that it has enforcement powers against companies that fail to make certain privacy statements for their European data.

While the Staff Paper is optimistic with respect to private dispute settlement mechanisms such as BBBOnline, the FTC's role remains a clear and important weakness in the enforcement mechanism. Rather than demand that the US prosecutes companies for these fundamental implementation deficiencies or challenge the continued existence of Safe Harbor, the paper choses only to identify these issues and to stress the European Commission's continued desire to work with the US government for future compliance. In effect, the paper reflects a significant political decision by the European Commission to avoid confrontation with the US over privacy issues at this juncture and to avoid revisiting the question of "adequacy". With the continuing threat of terrorism and the public focus on security, this choice defers a renewed debate on trans-Atlantic private sector data processing.

Continued on page 26

book reviews

Net Attitude: What it is, how to get it, and why your company can't survive without it

By John R. Patrick.
Perseus Publishing 2001,
ISBN 0-7382-0513-3 $26.00.
Reviewed by Eugene Oscapella

John Patrick, Vice President of Internet Technology at IBM Corporation, has written a highly readable and enthusiastic book about the perils and benefits of e-business. As the promotional material for the book asks, "why do so many businesses crash and burn when it comes to launching successful e-business strategies?"

Patrick argues that the inability to harness the full power of the Internet has much less to do with the technology itself than with the cultural and psychological barriers that straitjacket thinking about it.

The book should well be of interest to anyone considering stepping into the world of e-business. The book has a certain evangelical fervour to it (not uncharacteristic, it seems, of enthusiastic Internet "techies") but is highly readable nonetheless.

Of particular interest to PL&B readers is Patrick's chapter dealing with "trust". "Of all the issues that will affect the future of the Internet," he says, "safeguarding personal information is likely to be the most important because it is at the heart of trust. It means that information about an individual needs to be handled in a way that is consistent with the privacy and security expectations of the individual." If not, he says, there will be no trust.

The benefit for the reader of Patrick's chapter on trust lies in its detailed explanation of much of the mind-numbing vernacular dealing with security and privacy on the Internet. Patrick discusses a range of terms, from the ubiquitous Internet "cookies", to P3P, to digital IDs, authentication, authorisation, integrity and non-repudiation. For those who attend privacy, technology and security conferences and walk away with a splitting headache after trying to assimilate these concepts, this chapter alone justifies the book's price.

For those who perceive an increasing depersonalisation brought about by conducting business over the Internet, take hope. Patrick says that "people will have a lot of e-meetings, but I don't think people will give up on meeting in person as a result. There is too much that would be missed."

Further info: www.netattitude.org

E-Business Privacy and Trust

By Paul Shaw. Published by John Wiley & Sons Inc. 2001

Many companies are now looking to e-commerce as an additional channel for increasing revenue. But this potentially lucrative sector has its risks, and businesses who fail to understand and act upon issues of trust, privacy, and security could be leaving themselves open to lawsuits, negative publicity, and most importantly, decreasing revenue through the loss of customers.

E-Business and Trust is set out as a step-by-step handbook aiming to guide companies towards the correct privacy policy for their business. The book addresses many issues, such as consumer expectations, creating and communicating privacy policies, and outlining the legal aspects of maintaining privacy and security.

Written by an expert in computer law, and an author of a number of e-business publications, *E-Business and Trust*, is a relevant guide for both owners of small-scale startups and IT managers in larger companies.

Further info: www.wiley.com

Continued from page 9

As the Staff Paper reveals, the Safe Harbor has inherent flaws that are unlikely to disappear easily. US companies remain reluctant to join Safe Harbor. The implementation deficiencies show that strict compliance is elusive. At the same time, FTC sanctions for non-compliance are doubtful and private dispute settlements are still hypothetical. These fundamental issues will persist while Safe Harbor is used as a substitute for missing legal protections in the US.

In the interim, however, the strategy may to some extent improve US data protection for the treatment of European data by US companies. The Department of Commerce has modified the self-certification form in a way that partially implements FAQ 6 on human resources data. The European Commission's approach also gives US companies a second chance to try to implement the Safe Harbor principles. Companies, however, are at risk if they continue failing to properly implement Safe Harbor. The Staff Report notes specifically that only through "vigilance and enforcement action" can Safe Harbor be "credible and serve its purpose". Companies participating, and those contemplating joining, clearly have much work to do for satisfactory compliance. In addition, the response at the Member State level by the data protection supervisory authorities may not be as forgiving as this preliminary assessment by the European Commission. In any case, the European Commission is still required to make a full re-evaluation of Safe Harbor next year as mandated by Commission Decision 520/2000/EC.