US Companies Slow to Take Advantage of EU Directive Safe Harbour Agreement

Report by Rob Veeder

THE US DEPARTMENT OF COMMERCE finalised an informal "Safe Harbour" agreement with the EU in July 2000. Certifying to the Safe Harbour aims to offer assurance that your company provides 'adequate' privacy protection, as defined by the EU Directive.

According to the Department of Commerce, its purpose is to provide "an important way for US companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws" (PL&B Dec 00, p.9). As of early February, however, only the following 17 firms – few of them major entities – had signed on to Safe Harbour:

Adar International Inc., Crew Tags Int'l, Cybercitizens First, Decision Analyst Inc., Genetic Technologies Inc., HealthMedia Inc., Hewlett Packard, Numerical Algorithms Group, Privacy Leaders, Responsys, The Dun & Bradstreet Corporation, The USER-TRUST Network LLC, TRUSTe, United Information Group, USERFirst Inc., USERTrust Inc, WorldChoice-Travel.com Inc.

One reason for the lack of participation is that the agreement came into operation only in November 2000; companies have until the summer of 2000 to enter Safe Harbour. Thus, some companies have only just started to study the ramifications of Safe Harbour for their business activities. Others are biding time until they get answers to their questions about which data are covered. Still others are concerned about having potentially all their personal data processing activities subject to Federal Trade Commission enforcement scrutiny. They are attempting to develop contractual relationships that will allow them to comply with the EU Directive without such oversight.

Thus, 2001 raises many questions about the effect of Safe Harbour: Will the uncertainties about coverage be resolved? Will contractual arrangements be robust enough to suffice? Will the EU data protection forces target the non-compliant with enforcement actions in a still unsettled environment? And will the new US Congress spend time and resources resolving these kinds of privacy/data sharing issues? Stay tuned.

Continued from page 14

the same start-up compliance processes as Ms. Agress, Ms. Schacher noted that access to Walt Disney Internet Group sites is an opt-in process. They currently verify age using credit cards and are working on developing a gating system using technology to prevent those under 13 from having access without parental consent. They are also working to develop a system for verifiable parental consent. When Disney sites carry banner advertising, Disney requires these third party advertisers to be COPPA compliant as well.

Both presenters noted that complying with COPPA is an expensive proposition for most companies. There are the direct costs of setting up compliance processes and programmes. There are indirect costs as well, such as diverting resources from developing or carrying out other business activities. A company may simply decide to stop operating a website and forego the revenue it generated.

Is COPPA a model for Internet regulation? On the plus side, it forces data collectors to rationalise their need for data, makes them create internal programmes for managing such data and subjects them to oversight scrutiny. On the minus side, compliance is expensive. And until a way is found to distinguish the 12 year-old who has logged on from a 13 year-old, the law may not be able to achieve its intended purpose. And kids learn fast.

Rob Veeder is a Privacy Consultant and Director of The Privacy Advocates, 223 North Royal Street, Alexandria, VA 22314, USA
Tel: +1 703 548 5902,
E-mail: rveeder@flashcom.net