Two American initiatives to protect privacy on the Internet

Despite no signs of a comprehensive privacy law in the USA, there has been discussion about regulating the collection and use of personal data on the worldwide web, particularly when data is collected about children. Addressing the promotion and enhancement of privacy in cyberspace are two separate initiatives by Prof. Joel Reidenberg of Fordham University's School of Law, New York, and Susan Scott, Director of TRUST-e, Palo Alto, California.

Joel Reidenberg's project is to transform the "PICS" protocol for data protection purposes. PICS (the Platform for Internet Content Selection) was originally developed as a means of labelling World Wide Web sites according to their violent or pornographic content, and permitting users (primarily parents) to filter access to websites, so that children could be protected from Internet material suitable only for adults.

The WWW Consortium has set up a working group to develop a *Platform for Privacy Protection* (also known as P3) based on the PICS concept. To do so, data protection norms must be translated into P3 vocabularies. For instance, the practice of a website to collect personal data from users and sell it to any third party willing to pay for it might score 1 point, whereas the practice of collecting data and never disclosing to third parties could score 4 points. Then websites must be rated against this vocabulary. Finally, a user's web browser could be programmed to allow access only to those sites guaranteeing a certain level of privacy protection.

While undoubtedly innovative, there are, as Professor Reidenberg points out, some problems with the system. First, translating data protection norms into a P3 vocabulary simple enough to be understandable to the average Internet user is a complex process requiring value judgements to be made. Different competing vocabularies might emerge. Second is the issue of who carries out the rating of the websites. Self-reported ratings do not inspire the confidence of users, but if third parties are involved in the rating process, this adds to costs, particularly if there is a system of auditing websites' compliance with their stated privacy policies.

The TRUST-e initiative

Susan Scott's TRUST-e has developed just such a website rating system. For a fee, a website can submit an application to display a TRUST-e privacy label. To do so, a site must agree to: answer six mandatory questions regarding a site's information practices in site privacy statements; display a trustmark on its home page; adhere to stated privacy practices - even after termination from the program; and co-operate with all reviews and audits by TRUST-e.

The site's privacy statement must contain: what information is being gathered; what information will be used for; whom the information is being shared with; whether a user can opt-out; whether a user can correct or update a record; and whether a user can deactivate or remove a record.

Confidence in the ratings is ensured through a variety of tests carried out by TRUST-e's quality assurance process which includes: initial and periodic TRUST-e reviews; seeded information by TRUST-e; community monitoring; and third party random, on-site auditing by Coopers & Lybrand, KPMG Peat Marwick. Where a website's practices are shown *not* to match the requirements of the label which it has received, the website owner could be found guilty of breach of contract, a trademark infringement, or a fraudulent or deceptive practice. These enforcement remedies could be backed by the Federal Trade Commission.

However, there are worries that individual data subjects are not easily able to take action if they are the victim of a website whose privacy practices do not match up to its claims. A further criticism is that by relying on privacy labels or ratings and on the initiative of individual users to programme their browsers to block out sites, the system switches the responsibility for privacy protection away from the data controller and onto the data subject. In effect, if the data subject does not demand some privacy protection, he does not receive any. The end result is that there is no "bottom line" or minimum standard of privacy protection guaranteed for everybody.

However, such innovative solutions have a contribution to make towards the protection of privacy in cyberspace. A European rating and filtering system is also under consideration.

Report by Nick Platten independent consultant.