Microsoft settles with FTC over "Passport" system

By Eugene Oscapella

MICROSOFT HAS AGREED TO STEP UP its security practices and make them subject to a third-party compliance audit as part of a 20-year settlement with the US Federal Trade Commission (FTC).

The privacy enforcement action (settled August 8th) was brought against Microsoft last year following allegations that it misrepresented aspects of its Passport identification and authentication service.

The settlement also serves as a warning to other organisations of the need for accuracy when describing their privacy policies.

Microsoft's Passport portfolio is essentially a range of single sign-in services allowing web users to access sites without having to repeatedly log-in. The services vary according to the amount of data they collect. At its most basic level, Passport requires only an e-mail address and password for users to access websites which have signed up to the scheme. A secure purchasing service (Passport Wallet) collects and stores additional information such as credit card numbers and billing/delivery addresses, allowing consumers to buy goods and services from participating websites. A sign-in service for children (Kids Passport) has also been introduced, and is designed for parents who want to control how websites collect, process or disclose information on their children.

In July 2001, several consumer and privacy groups – including the Electronic Privacy and Information Center (EPIC), Junkbusters and the Electronic Frontier Foundation – filed a complaint with the FTC. In addition to the US actions, the European Commission is now examining whether Passport breached EU data protection laws (see *PL&B Int*, June 2002, p.2).

The FTC complaint alleged that Microsoft made false claims about the security of its Passport Wallet service, the level of privacy and security provided for personal information collected and stored by Passport, and its Kids Passport service. The complaint also alleged that Microsoft misrepresented claims that Passport did not collect any personal information (for example, data from web logs) other than that described in its privacy policy.

> ...the case should serve as notice to other Internet companies that make promises about privacy and security.

In particular, the FTC complained that Microsoft failed to implement and document procedures that were reasonable and appropriate to:

1. Preventing possible unauthorised access to the Passport system.

2. Detecting possible unauthorised access to the Passport system.

3. Monitoring the Passport system for potential vulnerabilities.

4. Recording and retaining system information sufficient to perform security audits and investigations.

The FTC concluded that Microsoft's claims of a high level of online security were "false or misleading".

Among other conditions, the FTC consent order prohibits Microsoft from misrepresenting its information practices "in any manner, expressly or by implication." Microsoft also must establish and maintain a comprehensive information security programme that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. This programme must contain safeguards appropriate to Microsoft's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers.

In addition, every two years Microsoft must have an independent professional certify its security programme as meeting or exceeding the standards in the consent order.

According to the *Washington Post*, FTC Chairman Timothy Muris and FTC Consumer Protection Bureau Director Howard Beales said the case should serve as notice to other Internet companies that make promises about privacy and security.

For more information see www.ftc.gov/opa/2002/08/microsoft.htm
For Microsoft's vision of "Trustworthy Computing", see p.16.