International Working Group
on Data Protection
in Telecommunications

675.31.10

Working Paper on Web browser caching of personal information in commercial and public multi-user web access environments (e.g. “Cybercafés”)

- adopted at the 38th meeting on 6-7 September 2005 in Berlin -[*]

1. Introduction

A cybercafé provides access to the Internet for a fee or free of charge. A similar free service is sometimes provided at public libraries and schools. In these shared environments, users communicate with family and friends, maintain contact with work and other commitments, and perform Internet banking and other money transfers. This makes cybercafés a target for criminals who steal personal information. With increasing awareness of the impact of ID theft, the role of the cybercafé operator is highlighted in helping to combat this problem.

2. Issues

Recent publicity given to ID theft and its impact on those affected highlights:

- risks associated with using the Internet for personal communication
- security issues in cybercafés
- inadequate housekeeping by cybercafé operators, which can jeopardize the personal information of users.

Client-side caching of information held in web pages has long been recognized as a security and possible privacy issue. Client-side caching involves the temporary storage of copies of web pages by web browsing software on the hard drive of a users’ own computer. All commonly installed web browsers use this technique e.g. it enables the use of a browser’s ‘back button’. It also saves return to the source of a previously downloaded web page if the page remains unchanged.

A security problem arises when personal information forms part of a web page cached by a web browser. The cached web page will, unless removed, remain on the user’s computer and may be available to other users by means of the browser back-button, history menu, and by direct search of the PC hard drive.

In cybercafés, a security issue arises at the end of a user session. Users who follow may be able to navigate to pages stored in the browser cache and access this information. There is a risk that in the light of publicity given to spyware and other malware, the security hazard presented by the browser cache has been overlooked.

[*] Due to national legislation Italy is not able to support the document.

3. Recommendation

Cybercafés should ensure that any personal information collected during a user session is completely removed after the end of that session (log-out). Furthermore the user himself should have the possibility to delete the content of the History folder before any other user is permitted to access the system. There should be a warning message/signal (e.g. a pop-up window) to draw the user's attention to delete the "History" before logging out.