from the original source, the more difficult it becomes to adhere to fair information practices.

6. Providers of e-mail systems should explore technical means to protect privacy

There are some technical measures which can be incorporated into e-mail systems to enhance privacy protection for users and other individuals who are subjects of e-mail messages.

The first line of defence against unauthorised access to e-mail is user identification through a unique identification number, bar code cards or smart cards and authentication through the use of passwords, hand prints or voice registration.

Encryption is another important technical means of protecting privacy. However, even if a local e-mail system is capable of encryption, the messages which are transferred to a public e-mail system are vulnerable to interception, as encryption is not usually available with public systems.

Other privacy protection features include the capacity to conceal the subject of a message and a warning that a message requiring special security has been received. Also, automatic log-off from the system, whenever the computer is inactive for a specified period of time, is another security feature which will help to prevent unauthorised access to e-mail.

Each organisation should examine its own security needs and select a system which is most appropriate for itself. An organisation's needs for security may vary depending on the type of information that is transmitted and received via e-mail.

7. Organisations should develop appropriate security procedures to protect e-mail messages

Technical features and privacy protection policies regarding e-mail will only be effective to the extent that they are accompanied by appropriate procedures to ensure the security of files and messages transmitted and received via e-mail.

This shortened version of the Ontario Information and Privacy Commissioner's report was edited by Bojana Bellmay, a *Privacy Laws and Business* consultant.

The full text of the report *Privacy Principles for Electronic Mail Systems* published by Tom Wright, Information and Privacy Commissioner, Ontario is available from his office. See page 25 for contact details.

FRANCE: VIDEO SURVEILLANCE UPDATE

Mme Louise Cadoux, vice president of the CNIL, France's Data Protection Authority, has called PL&B to give further information on our recent report (PL&B October '94 p. 17) on the CNIL's jurisdiction over video suveillance.

She stresses that CNIL claims jurisdiction over both digital and analogue video images captured and stored by any device. If a video image of a person is stored at all, the CNIL claims competence.

As stated in our report, the Senate debated the Public Security bill on November 8th and improved the text. However, the Senate rejected the CNIL's view of the extent of its competence over video surveillance.

A minimum of 60 members of the National Assembly may make an appeal to the Constitutional Court against this decision. But in the past, the court has said that a new law may modify the scope of a previous law. Therefore, the CNIL's view is unlikely to prevail along this route.