

## **E-MAIL DISCLAIMERS AND PRIVACY**

E-mail is active. The sender consciously communicates with an addressee, often many at once. E-mail is quick, with no easy chance to retrieve a message once sent. E-mails readily spread, with recipients able to copy and to forward to many other recipients, who may do the same and so on.

Securing communication via e-mail is a challenge for organisations. E-mail disclaimers are typically an attempt by organisations to meet the security challenge and reduce the adverse consequences of a breach. A disclaimer seeks to exclude or limit liability.

A well constructed e-mail disclaimer will invariably deal with several concerns, such as copyright, contract and tort issues.

Privacy often seems to be added to this list of concerns with insufficient thought to the privacy implications of sending personal information via e-mail. What follows is some advice to help organisations to consider how e-mail disclaimers may better address privacy concerns.

### **Why have a disclaimer?**

Privacy advice as part of an e-mail disclaimer can be a useful shorthand way of addressing requirements of three Information Privacy Principles:

IPP 4 requires organisations to take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;

IPP 5 requires organisations to document clearly expressed policies on management of personal information and provide the policies to anyone who asks;

IPP 6 gives individuals a right to seek access to their personal information and seek correction, mostly under the Victorian Freedom of Information Act.

### **Unencrypted e-mail is not secure**

Organisations should establish what personal information they are prepared to send via unencrypted (ie unprotected) e-mail. The more sensitive the personal information, the greater the risk.

Organisations should consider whether it is appropriate to send via e-mail material of a sensitive private nature because of the greater likelihood that the message will be read or intercepted by others whom it is not intended for.

A disclaimer does not prevent a message from being intercepted, nor being read by the wrong recipient nor in certain circumstances being used against the organisation in a court of law.

Ideally, organisations should conduct risk assessment to identify the extent to which they are prepared to use unencrypted e-mail.

### **Disclaimer content**

The content of e-mail disclaimers is important. They should be as brief as possible. In most cases, it should be sufficient to include :

- a warning to all recipients that the contents of the e-mail may contain personal information and that privacy should be respected at all times;

- a statement that the e-mail is intended for the addressee only and, if anyone else receives it, the steps that person should take (adapted appropriately to the context). For example, a disclaimer might say:
  - read only what is necessary to determine who the sender is and, if necessary in the circumstances, the subject of the personal information;
  - do not use, store, disclose, or copy the personal information that you were not intended to receive;
  - secure the personal information;
  - inform the sender that personal information has been misdirected; and
  - delete the personal information.

How the e-mail disclaimer appears on the e-mail is also important – automatically or at the discretion of employees. It is less risky to automatically embed the disclaimer.

Organisations may also choose to attach e-mail disclaimers to inter-agency e-mails. This is not yet common practice, but should be considered. For example, it is easy to see how a confidential e-mail could be sent to the wrong John Smith in the Victorian government when there are at least six individuals with this name.

## **Encryption**

Encryption is the process of systematically encoding data before transmission so that an unauthorised party cannot decipher it. There are different levels of encryption available. A risk assessment will help determine the strength of encryption required.

It is important to be wary of ‘out-of-the-box’ encryption, which will only work within an organisation’s own IT environment, rather than on all e-mail sent over the internet. To send encrypted e-mails over the internet, suitable arrangements

have to be made in advance with the addressees (there are various methods, such as the use of digital certificates). Organisations should consult their IT security manager.

## **Conclusion**

Securing personal information communicated via e-mail is part of the larger task of respecting privacy.

E-mail disclaimers are one precaution that organisations can use to try and minimise exposure to unauthorised access, use and disclosure.

Organisations should consider the risks and decide whether or not they want to send personal and sensitive information via unencrypted e-mail.

Ultimately, organisations should remember that marking a message 'private and confidential', whether on an envelope or an e-mail disclaimer, is not enough to guarantee delivery exclusively to the intended recipient.