

increased safeguards for personal information held in private sector databases.

If one card could make all payments and EFTPOS were universal, governments could employ the information generated to match individual income against expenditure.

Used in parallel with a system such as the proposed Australia card, there would be every opportunity for unobtrusive surveillance of citizens, unless there were stricter controls over the collection and use of such information.

The introduction of EFTPOS into retailing and banking, both of which are highly competitive industries, raises queries over the adequacy of consultation about the change.

ASTEC recommends further education for managers and union officials in information-sharing to encourage improved consultation practices.

Both industries employ large numbers of people who could be affected by the increasing automation of work which EFTPOS illustrates so vividly.

ASTEC also recommends the amount of work available in the banking and retail industries, and the trend to part-time and casual work, be studied to identify effects on individuals, households and the economy.

Customers using EFTPOS are now able to draw money from their accounts at a supermarket checkout. Such services, that are physically separate from banks, are likely to spread. Is a checkout operator also a bank teller in these circumstances?

Increased difficulty in differentiating between retailing and banking work could cause union demarcation problems, and suggests industrial relations issues that may need to be resolved.

EFTPOS will eventually affect us all if its growth continues. Yet few of us have had an opportunity to say whether it is a service we really want.

This suggests that better mechanisms for public awareness and consultation are needed.

The report gives examples of the advantages and disadvantages that consumers should weigh up.

ASTEC's intention in providing details of the disadvantages is not to be alarmist. It is instead to highlight the problems with electronic funds transfers that can be dealt with now before they grow too large.

This may allow the development of systems of payment that are better suited to consumers' needs.

"Who steals my PIN number..."

How secure is the PIN system?

Is it safe to put your money in the automatic bank teller machine? When will you be able to use one card for any transaction?

These were some of the issues canvassed at a recent meeting of the NSW Society for Computers and the Law.

In January 1986, a draft code of practice was sent by the NSW and Victorian Governments to financial institutions and consumer groups for their comments. The Commonwealth, too, is looking at ways to regulate the electronic transfer of funds.

Virginia Chadwick, MLC, wearing her hat as shadow minister for Consumer Affairs, told the Society both the NSW and Victorian draft guidelines differ in several areas from the Commonwealth draft. She expressed concern that such differences would lead away from the goal of uniformity of government policy on electronic funds transfer (EFT).

Ms Chadwick saw some points of contention in the NSW draft guidelines. Her major concerns were with ensuring the security of EFT and preventing irresponsible use of the cards themselves. For example, Section 4.1 of the guidelines lists seven points of information for inclusion on the receipts issued at teller machines. These are:

1. the amount of the transfer. Where the amount includes both an amount payable for goods or services and a cash advance, those amounts and the total amount shall be disclosed separately;
2. the date and, where possible, the time of transfer;
3. the kind of transfer, e.g. "deposit to savings", "transfer from savings to cheque account". Codes may be used only if explained on the receipt;
4. the codes identify the customer and the account being used;
5. the location of the terminal used by the customer, together with its identifying code;
6. the name of any third party to whom funds will be transferred; and
7. the account balance.

In Ms Chadwick's view, this is an excessive amount of information to be printed on the receipts, as security of the consumer's account could be breached.

An unscrupulous person could obtain

a receipt at the terminal and use that information for a dishonest purpose. She noted the Commonwealth report found that consumer groups were satisfied with the amount of information already provided on receipts.

Ms Chadwick believes voluntary regulation is preferable to a legislative solution.

Half of all EFT fraud involving teller machines happens in New York City, said Mr. Chris Riley from AUSTNET. He said the weakest point in the security of electronic transfers is the identification of cardholders by means of the personal identification number (PIN) and the card itself.

He was "amazed" that all the information necessary to produce a fake card is printed on all receipts.

Mr. Riley believes a partial solution to the problem of security is the use of message authentication codes. These are a secondary check of the identity of the user inside the teller machine.

Message codes provide proof the user had the key and also "prove within a probability which should be accepted by a court" that data has not been changed. Such message codes work unless a potential thief has the key.

Security is a problem which affects all kinds of electronic transfer of funds. Thieves have already stolen entire automatic teller machines. It is only a matter of time before someone steals the PIN pad used in shops to deduct money from accounts automatically.

Both teller machines and PIN pads contain the information necessary to access people's accounts.

Mr. Riley questioned the wisdom of relying on regulations to control the proliferation of different EFT systems and their possible abuse. In his opinion, because EFT is a technological system, political and bureaucratic supervision is inappropriate.

As an example, he cited the suggestion contained in the NSW draft guidelines that customers be allowed to choose their own PINs.

While it is easier for the customer to remember, the customer is likely to choose something obvious, like a birth-date, unless prevented.