



## PRIVACY MATTERS

---

August 2002

We should all be concerned about our privacy. After all, at a simple level most of us do not want to be bombarded with junk mail sent to us because someone has bought a mailing list with our name on it. And more seriously, we do not want unscrupulous operators to get hold of very personal information, such as credit card and banking details.

Security then is one issue, but so too is privacy and privacy has come into sharp focus with the passing of the latest Privacy Act in Australia which sets strict limits on what may be done with your personal information.

There is also an issue about employee and employer privacy, about what's acceptable for both parties to know and what is acceptable for them each to have access to.

Unfortunately, it seems that a good number of network administrators and the IT using community in general are not yet fully aware of the new privacy legislation and how it affects them.

Some of them may feel that they have a reasonable cause to be unconcerned because of the Act extending privacy to the private sector has not been tested in courts in relation to information technology. Not yet.

However, as well all know, in the eyes of the law ignorance is not bliss. Far from it. Quite simply, it is vitally important that anyone dealing with information about members of the public --- and let's face it that covers the majority of companies - should be aware of how the new privacy laws affect business and the way it's run.

Already, breaches of the Act have caused the collapse of at one high profile financial services company and it is odds on more companies will feel the force of the law if they do not ensure their staff know the requirements of the Act.

There are two broad dimensions to the privacy issue. The first is the need for network administrators to be aware of the privacy needs of an organization's customers or clients. The second are the privacy rights of your fellow employees.

### **Private concerns**

First, some background on the privacy provisions have been in place for federal government departments and organizations since 1988. At the end of December 2001, these were extended to include private organizations with a turnover of more than A\$3 million a year.

The new privacy sector provisions in the Privacy Act regulate the way many private sector organization collect, use, keep, secure and disclose personal information. Individuals now have the right to know what information an organization holds about them and a right to correct that information if it is wrong.

Coming hard on the heels of a major technology upgrade in industry generally to cope with fears of Y2K problems and the introduction of GST - the new privacy law was greeted with a collective yawn.

At the time the Act extended to the private sector, the Federal Privacy Commissioner estimated that as few as 19 per cent of Australian businesses had started preparing for the changes, despite the fact that they had 12 months to prepare got for the extension of the law.

Little has changed to shake Australian Business out of this lethargic state, according to many observers of the privacy issue.

However, attitudes are changing, they are having to – albeit slowly.

“What we’re finding is that as organizations build new systems, they are taking into account privacy,” says Mark Sercombe, partner in charge of the data privacy group at Deloitte Touche Tohmatsu. “We estimate it will take another five to seven years before industry is fully aware of privacy issues,” he adds Sercombe.

“One of the problems we see is that most business just don’t understand what privacy is and the Act and its guidelines are something of a patchwork quilt.”

That patchwork quilt came together as the government realized industry needed privacy legislation to give customers confidence in dealing with organizations mobbing into the digital economy.

Nigel Hutchinson, a former director of software giant SAP and now managing partner of legal firm Minerva, admits the arrival of privacy legislation for the It and data communications business has been, “a bit of a fizzer, it was largely a reaction to privacy legislation in what I would term socially friendly legal jurisdictions – such as those in Europe,” he says.

“The Australian government thought if we didn’t have similar laws on privacy, then the European would stop Australian companies doing business there. One of the issues is that most of us just don’t know if our privacy has been breached,” he Hutchinson.

“On top of this, organizations, such as the banks and insurance companies have had a good track record on this issue so most of us assume everybody else is being a good corporate citizen.”

Bernard Hill, the lead privacy consultant with 90East, a network services company with extensive federal government contracts, says organizations needs to understand the scope of the privacy legislation.

“It’s all about personal information from which a person’s identity can be obtained,”

Hill says. He added that on the networks monitored by 90East, there are about 1.4 million probes made each month by people looking to gain unauthorized access to data.

“That’s like someone rattling your door or windows to see if they’re open,” he says. “But 1.4 million a month means someone is doing it on average every two seconds. You need good security to track that and keep them out.”

In one famous privacy case, a financial services company simply dumped old records in past clients without even bothering to shred them. The company was held to have breached the privacy laws. The effect was devastating and eventually the company sadly had no other choice but to go into liquidation.

“One of the areas we see a potential problem is with companies acting as service providers,” Hutchinson adds. “They are handling data subject to privacy but are they doing sufficient to protect that data?”

This is likely to become a looming problem as more organizations switch to third parties for services such as data communications networks.

## **Private Services**

In a recent survey, research company Gartner found more than 60 per cent of financial service and telecommunication organizations in the Asia Pacific region have deployed IT utility services, including data communications, and the trend is increasing.

Gartner found adoption levels for IT utility services ranged from organizations spending less than US\$50,000 a year to those spending more than US\$1 million a year.

While it appears that many organizations are becoming more aware of the need to protect the data they hold on customers, there is some confusion on whether this extends to the information you hold on your fellow employees.

"We've had some classic enquires from clients," says Clark Butler, a partner with law firm Minter Ellison. "One client even asked if he had the right to access the C drive of an employee's PC. Absolutely – yes. The drive is part of a PC owned by the employer and connected to a network owned and operated by the employer.

"Fundamentally, employees do not have the right to privacy," Butler says, "but as with everything, network administrators need to adopt a cautious but commonsense approach."

He cited as example, a network manager noticing an employee sending emails to another employee inviting more than normal contact with each other...

"If the reply indicates an acceptance of the approach, then the network manager may be witnessing a case of sexual harassment and should take appropriate action," he says.

But when the action is appropriate and in what circumstances?

"With more and more people accessing the Internet and corresponding via email, it is vital that an organization has guidelines in place for their use," says Andrew Lysikatos, Vice President of Marketing for Zento, a company specializing in IT and communications security policy are more likely to have a proactive approach to the issues and part of the publicity listed Powelan Group.

"This gets back to the whole issue of security and privacy. Organizations to monitor the usage of shared electronic resources. WebSpy a Perth-based company is enjoying international success with its Email Analyzer. The company's CEO, Jack Andrys, believes 2002 will be the year in which companies increasingly acknowledge not only the importance of knowing what their bandwidth is being used for, but also the importance of good internal access control.

"It's a given that in today's modern-day office, people do, and should have email and Internet privileges," says Andrys. "But to protect against unscrupulous acts or dishonesty, companies need to protect have relevant software and indeed email usage policies in place. It's been shown that if email monitoring is done transparently, employees respond well and take a more responsible role in the management of the resource. More importantly they also go a long way in implementing good security procedures to handle the privacy of personal information."

## **HOW TO PROTECT PRIVACY**

- Security policy
- Security audit and risk assessment
- Security architecture and deployment

### **Security Policy**

The key to effective compliance with the Privacy Act is developing an organizational culture that respects privacy. "Organizations need to ensure that management and staff have a good information form misuse, loss, corruption or disclosure," says Andrew Lysikatos from Zento.

"One way to promote a respect for privacy would be to develop a security policy that would cover all organizational systems used for processing, storing, or transmitting personal information. The security risks faced by the organization could be assessed in the development of the policy, and then cost-effective measures decided to reduce the risks to acceptable levels. To be effective a security policy would need to be monitored and periodically reviewed. Staff and management would need to be made aware of the protective security policies and how to implement them.

### **Security audit and risk assessment**

Lysikatos says aspects to consider for IT security include physical security, computer and network security and communications security.

### **Security architecture and deployment**

Finally, if you are unsure, call in professional advice. "This can help in developing security policy through to developing a full security architecture and deploying it across your organization," Lysikatos says.

For more information go to <http://www.privacy.gov.au>

## ***Voice & Data Australia***