Privacy under siege
Karen Dearne
The Australian
JUNE 01, 2004

NIGHTMARE scenarios of citizens living under total surveillance are a possibility as technology gives governments the means to zip personal data together in a 21st-century form of the Australia Card, former Federal Privacy Commissioner Malcolm Crompton has warned. "There's a real risk that widespread use of lazy identity management solutions will make it technically easy to combine vast amounts of data about an individual without the person's knowledge or permission," Crompton told the AusCERT Asia-Pacific IT Security Conference at the Gold Coast last week.

"My concern is that this could amount to almost total surveillance of some - if not all - individuals," he says.

"We don't have to let it happen.

"The technology that's needed to protect our privacy is already available, it's public policy that is keeping it from being used.

"We must push for a debate now.

"It's extraordinarily important that we ensure protection of our own privacy and personal safety, rather than accepting what others want to push on us."

Citizens risk losing personal freedoms by degrees, Crompton says.

"It's the lobster-pot syndrome. Privacy problems arise as more and more data is put together, and also from function creep because of changed circumstances, such as terrorism. If data can be zipped together it eventually will be zipped together."

Avoiding the risks requires trust between consumers, business and government.

"Identity theft is the self-defeating consequence of increased demand for authentication: you don't trust me, so I won't trust you.

"If organisations don't get this right, there will be a backlash.

"People may change their behaviour in response to perceived scrutiny, and to prevent misunderstandings."

Businesses and governments should be using privacy-enhancing rather than privacy-invasive technologies, he says.

"The basic privacy principle is to only collect the information you need to authenticate a transaction," he says.

"Individuals should have control over who knows about them and how much they know.

"We are not building the transparency and accountability mechanisms that are needed."

Crompton advocates a multi-layer approach, with each person having a range of identifiers, possibly biometric, used in different applications - from the home or workplace to banking and contact with government agencies.
"Multiple IDs should be allowed, organisations should only authenticate when and what's necessary, unique identifiers should be specific to each application, and data should be kept in separate silos.

"Some biometrics should be ruled out because they include too much, or irrelevant, information.

"DNA should not be used as an identifier because it carries information about ethnic origin, health, and families; speech recognition systems can also convey more information than you would expect."

Karen Dearne attended AusCERT2004 on the Gold Coast as a guest of AusCERT.

This report appears on australianIT.com.au.